MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

ZZ校跑 1.0.1.APK

APP名称:	ZZ校跑
包名:	zzpaotui.paotuisylg.client
域名线索:	40条
URL线索:	85条
邮箱线索:	0条
分析日期:	2022年1月20日 22:30

文件信息

文件名: zzxiaopao.apk
文件大小: 17.82MB
MD5值: b09c8dee11248c6bc4ada2ab3c483f70
SHA1值: 09f88908162e44ef8a994a28b15d3783584f3a49
SHA256值: e10fe6834bb39b9fec339077ded97804a4ff8611853d13b8742b11dbc514b97a

APP 信息

App名称: ZZ校跑
包名: zzpaotui.paotuisylg.client
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0.1
安卓版本: 101

域名线索

域名	是否危险域名	服务器信息
wprd0d.is.autonavi.com	good	没有服务器地理信息.
lbs.amap.com	good	**IP:** 59.82.29.156 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
mcgw.alipay.com	good	IP: 203.209.250.50 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
cgicol.amap.com	good	IP: 59.82.60.45 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.
mclient.alipay.com	good	IP: 203.209.250.50 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
mobilegw.alipay.com	good	IP: 203.209.255.238 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
loggw-exsdk.alipay.com	good	IP: 110.76.3.2 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
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
xmlpull.org	good	IP: 74.50.62.60 所属国家: United States of America 地区: Texas 城市: Dallas 纬度: 32.814899 经度: -96.879204 查看地图: Google Map
wb.amap.com	good	IP: 59.82.31.156 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
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
apiinit.amap.com	good	IP: 106.11.43.113 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
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
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
adiu.amap.com	good	IP: 59.82.31.202 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
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
mobilegw.stable.alipay.net	good	没有服务器地理信息.
yuntuapi.amap.com	good	没有服务器地理信息.
mobilegw.alipaydev.com	good	**IP:** 110.75.132.131 **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
wappaygw.alipay.com	good	**IP:** 203.209.250.6 **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
abroad.apilocate.amap.com	good	IP: 59.82.39.53 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
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
m.alipay.com	good	IP: 203.209.245.74 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
wap.amap.com	good	IP: 42.202.208.240 所属国家: China 地区: Liaoning 城市: Chaoyang 纬度: 40.457420 经度: 123.550629 查看地图: Google Map
restsdk.amap.com	good	IP: 203.119.175.194 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
dualstack-a.apilocate.amap.com	good	IP: 106.11.40.50 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
h5.m.taobao.com	good	IP: 59.47.225.233 所属国家: China 地区: Liaoning 城市: Benxi 纬度: 41.288609 经度: 123.764999 查看地图: Google Map

域名	是否危险域名	服务器信息
mpsapi.amap.com	good	IP: 106.11.43.68 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
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
m5.amap.com	good	IP: 106.11.35.98 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
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

域名	是否危险域名	服务器信息
api.weixin.qq.com	good	**IP:** 81.69.216.43 **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
mobilegw.aaa.alipay.net	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
apilocate.amap.com	good	**IP:** 59.82.60.15 **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
render.alipay.com	good	**IP:** 116.95.26.243 **所属国家:** China **地区:** Nei Mongol **城市:** Chifeng **纬度:** 42.268330 **经度:** 118.963608 **查看地图:** Google Map

域名	是否危险域名	服务器信息
dualstack-arestapi.amap.com	good	IP: 39.98.22.142 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
https://render.alipay.com/p/s/i?scheme=%s	com/alipay/sdk/app/OpenAuthTask.java
https://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://wappaygw.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/service/rest.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
http://mclient.alipay.com/home/exterfaceAssign.htm	com/alipay/sdk/app/PayTask.java
https://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java

URL信息	Url所在文件
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/cons/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/cons/a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/data/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/loc/cc.java
http://restsdk.amap.com	com/loc/s.java

URL信息	Url所在文件
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/loc/ef.java
http://restsdk.amap.com/v3/geocode/regeo	com/loc/ef.java
https://restsdk.amap.com/v3/iasdkauth	com/loc/l.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/loc/l.java
http://apilocate.amap.com/mobile/binary	com/loc/ek.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ek.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/ed.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/eo.java
http://restsdk.amap.com/v3/place/text?	com/loc/a.java
http://restsdk.amap.com/v3/config/district?	com/loc/a.java
http://restsdk.amap.com/v3/place/around?	com/loc/a.java
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://mpsapi.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java

URL信息	Url所在文件
http://m5.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/amap/mapcore/maploader/AMapLoader.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/autonavi/amap/mapcore/Inner_3dMap_location.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	com/amap/api/mapcore/util/b.java
http://restsdk.amap.com/v4/grasproad/driving?	com/amap/api/mapcore/util/ge.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/mapcore/util/du.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/mapcore/util/du.java
http://restsdk.amap.com	com/amap/api/mapcore/util/gs.java
http://apiinit.amap.com/v3/log/init	com/amap/api/mapcore/util/gl.java
https://adiu.amap.com/ws/device/adius	com/amap/api/mapcore/util/ij.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/mapcore/util/gk.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/mapcore/util/gk.java
http://apilocate.amap.com/mobile/binary	com/amap/api/mapcore/util/ke.java

URL信息	Url所在文件
http://dualstack-a.apilocate.amap.com/mobile/binary	com/amap/api/mapcore/util/ke.java
http://restsdk.amap.com/v4	com/amap/api/mapcore/util/dg.java
http://restsdk.amap.com/v4	com/amap/api/mapcore/util/i.java
http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0	com/amap/api/col/s/bf.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/col/s/bf.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/col/s/bf.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/col/s/bf.java
http://restsdk.amap.com/v3	com/amap/api/col/s/h.java
https://restsdk.amap.com/v3	com/amap/api/col/s/h.java
http://restsdk.amap.com/v4	com/amap/api/col/s/h.java
https://restsdk.amap.com/v4	com/amap/api/col/s/h.java
http://yuntuapi.amap.com	com/amap/api/col/s/h.java
https://yuntuapi.amap.com	com/amap/api/col/s/h.java
http://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/s/h.java
https://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/s/h.java

URL信息	Url所在文件
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/s/h.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/s/h.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/s/bk.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/s/bj.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/s/bj.java
https://adiu.amap.com/ws/device/adius	com/amap/api/col/s/cr.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
http://wap.amap.com/	com/amap/api/maps/AMapUtils.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
https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java

URL信息	Url所在文件
https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s	io/dcloud/feature/oauth/weixin/WeiXinOAuthService.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
http://lbs.amap.com/api/android-sdk/guide/error/	io/dcloud/js/map/amap/adapter/AMapLink.java
https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/f/b/c.java
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

URL信息	Url所在文件
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://mpsapi.amap.com/ws/mps/vmap	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://mpsapi.amap.com/ws/mps/rtt	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://mpsapi.amap.com/ws/mps/smap	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://mpsapi.amap.com/	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.so
http://m5.amap.com	lib/armeabi-v7a/libAMapSDK_MAP_v7_9_1.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.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.ACCESS_SURFACE_FLINGER	合法	访问 SurfaceFlinger	允许应用程序使用 SurfaceFlinger 低级功能

向手机申请的权限	是否危险	类型	详细情况
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
android.permission.MEDIA_CONTENT_CONTROL	正常		允许应用程序知道正在播放什么内容并控制其播放
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

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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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: CN=bytedance
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2017-12-28 02:08:43+00:00
Valid To: 2042-12-22 02:08:43+00:00
Issuer: CN=bytedance
Serial Number: 0x5bc7149
Hash Algorithm: sha256
md5: aea76db732199caed712e47dcb444448
sha1: 453bc7b729a09ba6b3d7f659be53ed1fd996e1d6
sha256: 2223ef5272b062b248fcca56922b51b3d91434a4b6789fe7fb0f59ddb6ba4443
sha512: 7101d0ee7bb5580606cd42a5619a41b5d1586319f7cf9a13c8fc3bd2a3bf639cc9ed8f6f232db9ced74f4576c92653b5bbec3bed9b9447fb06896e79ca47a8b4
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 936a32deb1d972cde9b21cfa94611602ca0a7b42d7443f7423b7ca243754c7de

Exodus威胁情报

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

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_oauth_weixin_plugin_description" : "wechat"
"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"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_feature_oauth_weixin_plugin_description" : "微信"
"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"

可能的敏感信息
"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

文件列表	分析结果
classes.dex	<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.PRODUCT check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check device ID check subscriber ID check ro.product.device check ro.kernel.qemu check emulator file check possible VM check</td></tr><tr><td>编译器</td><td>r8</td></tr></table>

<table>
<tr><th>文件列表</th><th>分析结果</th></tr>
<tr><td>classes2.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</td></tr>
<tr><td>编译器</td><td>r8 without marker (suspicious)</td></tr>
</table>
</td></tr>
</table>
