MoGua

172号卡 1.5.0.APK 分析报告

APP名称: 172号卡

包名:	com.canghai.haoka
域名线索:	69条
URL线索:	62条
邮箱线索:	1条
分析日期:	2025年1月15日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 12_base.apk
文件大小: 27.6MB
MD5值: 2bcb568bd79ea7f410bc1a2f86aa7441
SHA1值: 11abb51410989175d2c3e5b42a0bf6c5cc66a7b6
SHA256值: 33b39311446f606871a9bfb5ffab57e0ff2059a030ab901bed298caeab75e3a4

APP 信息

App名称: 172号卡
包名: com.canghai.haoka
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.5.0
安卓版本: 150

域名线索

域名	服务器信息
metrics1-drcn.dt.dbankcloud.cn	**IP**: 111.202.16.252 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
er.dcloud.net.cn	**IP**: 43.142.131.213 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.cn	**IP**: 49.4.40.185 **所属国家**: China **地区**: Guangdong

	城市: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
norma-external-collect.meizu.com	IP: 183.60.176.112 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
open.weixin.qq.com	IP: 220.196.154.28 **所属国家**: China **地区**: Jiangsu **城市**: Wuxi **纬度**: 31.569349 **经度**: 120.288788
er.dcloud.io	没有服务器地理信息.
metrics2.data.hicloud.com	IP: 80.158.38.48 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
uniapp.dcloud.net.cn	IP: 101.72.254.86 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
log.tbs.qq.com	IP: 124.95.231.218 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877

api-push.in.meizu.com	**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
grs.dbankcloud.eu	没有服务器地理信息.
m3w.cn	**IP**: 119.188.149.190 **所属国家**: China **地区**: Shandong **城市**: Jinan **纬度**: 36.668331 **经度**: 116.997223
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
haoka.lot-ml.com	**IP**: 101.67.15.14 **所属国家**: China **地区**: Zhejiang **城市**: Lishui **纬度**: 28.460419 **经度**: 119.909721
api-push.meizu.com	**IP**: 221.5.93.66 **所属国家**: China **地区**: Guangdong **城市**: Foshan **纬度**: 23.026770 **经度**: 113.131477
	IP: 31.13.94.37

www.google.com	**所属国家**: Argentina **地区**: Ciudad Autonoma de Buenos Aires **城市**: Buenos Aires **纬度**: -34.603600 **经度**: -58.381554
d-gt.getui.com	没有服务器地理信息.
eid.faceid.qq.com	**IP**: 60.28.172.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
metrics5.data.hicloud.com	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
www.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
ask.dcloud.net.cn	**IP**: 115.56.90.192 **所属国家**: China **地区**: Henan **城市**: Jiaozuo **纬度**: 35.239719 **经度**: 113.233063
	IP: 60.28.172.40 **所属国家**: China

tbsrecovery.imtt.qq.com	**地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
b-gtc.getui.nethttps	没有服务器地理信息.
data-dre.push.dbankcloud.com	**IP**: 80.158.49.244 **所属国家**: Germany **地区**: Schleswig-Holstein **城市**: Kiel **纬度**: 54.321358 **经度**: 10.134532
cn.register.xmpush.xiaomi.com	**IP**: 123.125.102.39 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
data-drru.push.dbankcloud.com	**IP**: 159.138.202.31 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
tbs.imtt.qq.com	**IP**: 101.69.99.73 **所属国家**: China **地区**: Zhejiang **城市**: Huzhou **纬度**: 30.870550 **经度**: 120.093300
schemas.android.com	没有服务器地理信息.
	IP: 114.247.154.13 **所属国家**: China

resolver.msg.xiaomi.net	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
172appapi.lot-ml.com	**IP**: 101.67.15.14 **所属国家**: China **地区**: Zhejiang **城市**: Lishui **纬度**: 28.460419 **经度**: 119.909721
api.bspapp.com	**IP**: 39.96.249.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
c-gtc.getui.nethttps	没有服务器地理信息.
haokaapi.lot-ml.com	**IP**: 101.67.15.14 **所属国家**: China **地区**: Zhejiang **城市**: Lishui **纬度**: 28.460419 **经度**: 119.909721
10.38.162.35	**IP**: 10.38.162.35 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
haokawx.lot-ml.com	**IP**: 101.67.15.14 **所属国家**: China **地区**: Zhejiang **城市**: Lishui

	纬度: 28.460419 **经度**: 119.909721
service.dcloud.net.cn	**IP**: 110.40.169.99 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mlhaoka.supremesoft.cn	**IP**: 211.149.152.236 **所属国家**: China **地区**: Sichuan **城市**: Chengdu **纬度**: 30.666670 **经度**: 104.066269
mdc.html5.qq.com	**IP**: 125.39.196.199 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
data-dra.push.dbankcloud.com	**IP**: 119.8.163.189 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
mqqad.html5.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 94.74.88.100

metrics-dra.dt.hicloud.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
grs.platform.dbankcloud.ru	没有服务器地理信息.
sdk-open-phone.getui.com	**IP**: 101.68.218.167 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199 **经度**: 120.750000
metrics5.dt.dbankcloud.ru	**IP**: 159.138.203.215 **所属国家**: Russian Federation **地区**: Sverdlovskaya oblast' **城市**: Yekaterinburg **纬度**: 56.857498 **经度**: 60.612499
zxid-m.mobileservice.cn	**IP**: 101.69.207.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
mlappapi.supremesoft.cn	**IP**: 211.149.152.236 **所属国家**: China **地区**: Sichuan **城市**: Chengdu **纬度**: 30.666670 **经度**: 104.066269
gtc.getui.nethttps	没有服务器地理信息.
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
kf.qq.com	**IP**: 140.207.124.86 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
long.open.weixin.qq.com	**IP**: 112.65.193.150 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
eid-enhance.faceid.qq.com	**IP**: 116.130.229.78 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
apis.map.qq.com	**IP**: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
c-hzgt2.getui.com	**IP**: 124.160.155.61 **所属国家**: China **地区**: Zhejiang **城市**: Jiaxing **纬度**: 30.752199

	经度: 120.750000
quilljs.com	**IP**: 172.66.43.93 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
xml.org	**IP**: 104.239.240.11 **所属国家**: United States of America **地区**: Texas **城市**: Windcrest **纬度**: 29.499678 **经度**: -98.399246
pms.mb.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
api.weixin.qq.com	**IP**: 116.128.184.169 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
debugx5.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
	IP: 121.36.117.8 **所属国家**: China **地区**: Beijing

data-drcn.push.dbankcloud.com	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
grs.dbankcloud.asia	**IP**: 49.4.35.251 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
xmlpull.org	**IP**: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.qq.com	**IP**: 221.198.70.47 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
debugtbs.qq.com	**IP**: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
cfg.imtt.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102

grs.dbankcloud.com	**IP**: 60.28.193.195 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
faceid-ecard-1254418846.cos.ap-chengdu.myqcloud.com	**IP**: 58.144.165.245 **所属国家**: China **地区**: Chongqing **城市**: Chongqing **纬度**: 29.562780 **经度**: 106.553101
aid.mobileservice.cn	**IP**: 101.69.207.68 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
ns.adobe.com	没有服务器地理信息.
api.next.bspapp.com	**IP**: 203.107.60.33 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL**信息**	Url**所在文件**
https://c-gtc.getui.net,https://c-gtc.gepush.com	com/getui/gtc/c/b.java

https://gtc.getui.net,https://gtc.gepush.com	com/getui/gtc/c/b.java
https://b-gtc.getui.net,https://b-gtc.gepush.com	com/getui/gtc/c/b.java
https://sdk-open-phone.getui.com/	com/getui/gtc/i/d/b.java
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/namespace-prefixes	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-general-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/external-parameter-entities	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xml.org/sax/features/string-interning	com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html	com/huawei/secure/android/common/xml/XmlNewPullParserSecurity.java
http://xmlpull.org/v1/doc/features.html	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xml.org/sax/features/namespaces	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
http://xml.org/sax/features/validation	com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java
https://sdk-open-phone.getui.com/api.php	com/igexin/push/a.java
https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java
https://d-gt.getui.com/api.htm	com/igexin/push/a.java
https://bi.	com/igexin/push/config/b.java
https://config.	com/igexin/push/config/b.java

https://bi.	com/igexin/push/config/g.java
https://config.	com/igexin/push/config/g.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/server/getPushConf	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.in.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/constants/PushConstants.java
https://api-push.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/c/a.java
https://api-push.in.meizu.com/garcia/api/client/	com/meizu/cloud/pushsdk/platform/c/a.java
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/cloud/pushsdk/platform/c/a.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.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://debugtbs.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugx5.qq.com	com/tencent/smtt/sdk/WebView.java
https://debugtbs.qq.com?10000\	com/tencent/smtt/sdk/WebView.java
https://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/l.java

https://mdc.html5.qq.com/d/directdown.jsp?channel_id=50079	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/stat/MttLoader.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/ui/dialog/d.java
https://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/ui/dialog/d.java
https://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/o.java
https://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/o.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/o.java
https://tbsrecovery.imtt.qq.com/getconfig	com/tencent/smtt/utils/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com/tencent/smtt/utils/d.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/hh.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/hz.java
https://%1$s/gslb/?ver=5.0	com/xiaomi/push/dd.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/ia.java

http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/gv.java
http://10.38.162.35:9085	com/xiaomi/push/service/v.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/v.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bx.java
https://aid.mobileservice.cn/	com/zx/a/I8b7/q2.java
https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/I8b7/h.java
https://zxid-m.mobileservice.cn/sdk/app/depAnalysis	com/zx/a/I8b7/r0.java
https://zxid-m.mobileservice.cn/sdk/module/getCoreModule	com/zx/a/I8b7/v.java
https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken	com/zx/a/I8b7/f1.java
https://zxid-m.mobileservice.cn/sdk/extend/tag	com/zx/a/I8b7/j1.java
https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/I8b7/g1.java
https://zxid-m.mobileservice.cn/sdk/channel/report	com/zx/a/I8b7/z0.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/e/b/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/e/b/a.java
https://er.dcloud.io/rv	io/dcloud/e/c/h/c.java

https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/c.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/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
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
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/g/b.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.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
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://data-drcn.push.dbankcloud.com	摸瓜V2引擎
https://data-dra.push.dbankcloud.com	摸瓜V2引擎
https://data-dre.push.dbankcloud.com	摸瓜V2引擎

https://data-drru.push.dbankcloud.com	摸瓜V2引擎
https://metrics1-drcn.dt.dbankcloud.cn:443	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.dt.dbankcloud.ru:6447	摸瓜V2引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://grs.platform.dbankcloud.ru	摸瓜V2引擎
https://grs.dbankcloud.eu	摸瓜V2引擎
https://github.com/uuidjs/uuid	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=$	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quilljs.com/	摸瓜V2引擎

https://quilljs.com	摸瓜V2引擎
https://haoka.lot-ml.com/zhuce.html\	摸瓜V2引擎
https://haoka.lot-ml.com/yinsizhengce.html\	摸瓜V2引擎
https://api.next.bspapp.com	摸瓜V2引擎
https://api.bspapp.com	摸瓜V2引擎
https://$	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/secure-network.html	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise	摸瓜V2引擎
https://mlhaoka.supremesoft.cn/view/system/faceresult.html	摸瓜V2引擎
https://faceid-ecard-1254418846.cos.ap-chengdu.myqcloud.com/eidLogo.png	摸瓜V2引擎
https://kf.qq.com/	摸瓜V2引擎
http://www.qq.com/privacy.htm	摸瓜V2引擎
https://mlappapi.supremesoft.cn/ewm_bg.png	摸瓜V2引擎
https://haokawx.lot-ml.com/h5order/index?pudID=$	摸瓜V2引擎
https://haokawx.lot-ml.com/h5order/index?pudID=	摸瓜V2引擎
https://haokawx.lot-ml.com/PackInfo/Detail/	摸瓜V2引擎
https://haokawx.lot-ml.com/Product/index/	摸瓜V2引擎
https://haokawx.lot-ml.com/Product/Shop/	摸瓜V2引擎

https://haokawx.lot-ml.com/GetWx/Index?UserID=	摸瓜V2引擎
https://haoka.lot-ml.com/zhuce.html	摸瓜V2引擎
https://haoka.lot-ml.com/yinsizhengce.html	摸瓜V2引擎
https://172appapi.lot-ml.com/	摸瓜V2引擎
https://haokaapi.lot-ml.com/	摸瓜V2引擎
https://eid.faceid.qq.com	摸瓜V2引擎
https://eid-enhance.faceid.qq.com	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
将您的问题发送至dataprivacy@tencent.com或寄到如下地址	摸瓜V2引擎

手机线索

手机号	所在文件
	com/tencent/smtt/sdk/o.java

18222222222	
15907417083	摸瓜V1引擎

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=, L=, O=Android, OU=Android, CN=n3xg%2FiNkTaYDA1nT1Bvc8a4DSsVl1fNU5CMOfM1d9QTj1Lps6sryZOkbAQXQDlST
签名算法: rsassa_pkcs1v15
有效期自: 2023-09-27 05:19:06+00:00
有效期至: 2123-09-03 05:19:06+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=n3xg%2FiNkTaYDA1nT1Bvc8a4DSsVl1fNU5CMOfM1d9QTj1Lps6sryZOkbAQXQDlST
序列号: 0x26154fde
哈希算法: sha256
md5值: 6a70138b35f8d8b7c2d2664d18301ad9
sha1值: b04d029461125be3059b4fb34b6f0c56f6c10f7d
sha256值: 6bff5c3ad95a327d0e282913c5eab0fe71cc236ae4935d42c236e1edd4f7b0e9
sha512值: bdbf7751d2f684e60ca743e3dcf430fbf63d7c620b60bfdb38b9cfff3528cb57f4f6e24acfdafb13e9fdf602755c35d5570ee07b0ee2311bfc5c11c3e61066e8
公钥算法: rsa
密钥长度: 2048
指纹: bb86774d16bca620922088fe263e2afd9d35b51798c4c5d78a8397dd4aa53bd8

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_tips_certificate" : "certificate"

"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"

"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"

"dcloud_tips_certificate" : "证书"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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
	正		

android.permission.ACCESS_NETWORK_STATE	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.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.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.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	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

	险		
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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未	Unknown	Unknown permission from android reference

	知	permission	
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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	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
getui.permission.GetuiService.com.canghai.haoka	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作
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_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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
com.canghai.haoka.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
com.canghai.haoka.permission.PUSH_PROVIDER	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
com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.canghai.haoka.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
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.canghai.haoka.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
com.canghai.haoka.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

com.hihonor.push.permission.READ_PUSH_NOTIFICATION_INFO	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: unipush://, Hosts: io.dcloud.unipush, Paths: /,

---