



MoGua

慧生活798 1.0.133.APK 分析报告



APP名称:	慧生活798
包名:	com.cloudora.android
域名线索:	64条
URL线索:	66条
邮箱线索:	3条

分析日期:2024年5月7日

分析平台:[摸瓜反编译平台](#)

文件信息

文件名: hnkzy.apk
文件大小: 45.82MB
MD5值: 09248879962905ae9b35535f49f832e8
SHA1值: 2a6b7a9e1c1c71e5ec525a2fe6929ddbc72f992a
SHA256值: 7844bf07b4fd070e65f033b112e83ab0613246c8dc09c62a44053a9766ab5113

APP 信息

App名称: 慧生活798
包名: com.cloudora.android
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0.133
安卓版本: 1133

域名线索

域名	服务器信息
	IP: 101.68.218.173 所属国家: China 地区: Zhejiang

sdk-open-phone.getui.com	城市: Jiaxing 纬度: 30.752199 经度: 120.750000
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
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
www.csjplatform.com	IP: 42.236.86.222 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
p1-lm.adkwai.com	IP: 125.38.214.76 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
apps.bytesfield.com	IP: 182.40.61.214 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
ask.dcloud.net.cn	IP: 123.125.244.13 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
service.dcloud.net.cn	IP: 124.220.57.196 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

mcgw.alipay.com	IP: 123.125.216.242 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
act2.hnkzy.com	IP: 106.14.24.158 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
wappaygw.alipay.com	IP: 123.125.216.241 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
webcast.amemv.com	IP: 61.182.131.172 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
apps.bytesfield-b.com	IP: 42.236.86.220 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
cloud.hnkzy.com	IP: 47.101.184.29 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.cmbchina.com	IP: 210.22.252.24 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
wallet.95516.com	IP: 125.44.163.89 所属国家: China 地区: Henan 城市: Nanyang 纬度: 32.994720

	经度: 112.532784
apps.oceanengine.com	IP: 182.40.60.214 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
mclient.alipay.com	IP: 125.39.43.133 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
i.snssdk.com	IP: 61.182.131.160 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
static.yximgs.com	IP: 119.188.131.35 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
partner.toutiao.com	IP: 121.29.30.187 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
mobilegw.alipaydev.com	IP: 110.75.132.131 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.thorui.cn	IP: 119.91.210.224 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dl.hnkzy.com	IP: 106.14.24.158 所属国家: China 地区: Shanghai

	城市: Shanghai 纬度: 31.224333 经度: 121.468948
developer.huawei.com	IP: 42.236.84.33 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
zxid-m.mobileservice.cn	IP: 101.69.207.69 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
u.kuaishou.com	IP: 103.102.202.80 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mobilegw.alipay.com	IP: 203.209.243.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
docs.getui.com	IP: 124.160.116.170 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.fresco-cn.org	IP: 8.212.40.144 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
privacy.oppo.com	IP: 61.162.100.108 所属国家: China 地区: Shandong 城市: Zibo 纬度: 36.790775 经度: 118.063354
schemas.android.com	没有服务器地理信息.

privacy.qq.com	IP: 124.163.196.157 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
er.dcloud.io	没有服务器地理信息.
union.baidu.com	IP: 111.206.208.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
rule.tencent.com	IP: 120.221.152.206 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
www.google.com	IP: 69.50.221.20 所属国家: United States of America 地区: Arizona 城市: Phoenix 纬度: 33.682438 经度: -112.107254
www.wechat.com	IP: 43.153.248.110 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
c-hzgt2.getui.com	IP: 124.160.155.59 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
apps.samsung.com	IP: 111.161.120.36 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
	IP: 106.14.125.42 所属国家: China

i.hnkzy.com	地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.msa-alliance.cn	IP: 106.75.146.79 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
render.alipay.com	IP: 125.39.47.200 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
i.ilife798.com	IP: 47.101.162.231 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
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
h5.m.taobao.com	IP: 125.39.103.206 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
loggw-exsdk.alipay.com	IP: 110.76.3.2 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
d-gt.getui.com	没有服务器地理信息.
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271

	经度: -121.988571
open.weixin.qq.com	IP: 223.167.82.219 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.samsungapps.com	IP: 52.31.24.56 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
mobilegwpre.alipay.com	IP: 110.75.138.35 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
sf6-ttcdn-tos.pstatp.com	IP: 103.3.115.129 所属国家: China 地区: Zhejiang 城市: Taizhou 纬度: 28.666668 经度: 121.349998
ns.adobe.com	没有服务器地理信息.
weexapp.com	IP: 203.119.169.98 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
m3w.cn	IP: 120.221.152.183 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223

e.qq.com	IP: 220.194.116.85 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
open.e.kuaishou.com	IP: 116.136.162.35 所属国家: China 地区: Nei Mongol 城市: Hohhot 纬度: 40.810650 经度: 111.650665
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
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
netpay.cmbchina.com	IP: 58.33.159.101 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
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
act.hnkzy.com	IP: 106.14.24.158 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

URL信息	Url所在文件
http://cmbbls/	cmbapi/CMBApiEntryActivity.java
https://cmbbls/	cmbapi/CMBApiEntryActivity.java
https://mobilegwpre.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
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
http://mclient.alipay.com/cashier/mobilepay.htm	com/alipay/sdk/app/PayTask.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/m/l/a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/m/l/a.java
https://loggw-exsdk.alipay.com/loggw/logUpload.do	com/alipay/sdk/m/l/a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/m/l/a.java
https://h5.m.taobao.com/mlapp/olist.html	com/alipay/sdk/m/m/a.java
https://webcast.amemv.com/falcon/webcast_douyin/page/anchor_task_v2/panel/index.html?web_bg_color=%23ff161823	com/bytedance/android/live/base/api/BuildConfig.java
https://webcast.amemv.com/falcon/webcast_douyin/page/recharge_v1/index.html	com/bytedance/android/live/base/api/BuildConfig.java
https://i.snssdk.com/	com/bytedance/sdk/openadsdk/downloadnew/core/AdBaseConstants.java

https://sdk-open-phone.getui.com/	com/getui/gtc/i/d/b.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.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://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/adLive/ks_so-adLiveNoSoRelease-3.3.59-5a16210b94-483.zip	com/kwad/components/offline/a/b.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArm64v8aRelease-3.3.44.2-e8fbb3a5f8-666.apk	com/kwad/components/offline/a/a/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/adLive/ks_so-adLiveArmeabiv7aRelease-3.3.44.2-e8fbb3a5f8-666.apk	com/kwad/components/offline/a/a/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/obiwan/ks_so-obiwanNoSoRelease-3.3.56-445ef4f109-409.zip	com/kwad/components/offline/b/b.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/offline_components/tk/ks_so-tachikomaNoSoRelease-3.3.61-f6023045dd-499.zip	com/kwad/components/offline/c/c.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_lite_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v8_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_lite_3358	com/kwad/components/offline/c/b/a.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/tachikoma/3.3.58/ks_tk_so_v7_3358	com/kwad/components/offline/c/b/a.java
https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties	com/kwad/framework/filedownloader/services/a.java
https://open.e.kuaishou.com/rest/e/v3/open/sdk2	com/kwad/sdk/api/loader/u.java
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArm64v8aRelease-3.3.14.apk	com/kwad/sdk/collector/d.java
https://static.yximgs.com/udata/pkg/KS-Android-KSAdSDK/ks_so-appStatusArmeabiv7aRelease-3.3.14.apk	com/kwad/sdk/collector/d.java
http://%s:%d/%s	com/kwad/sdk/core/videoCache/f.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/kwad/sdk/core/videoCache/h.java

https://github.com/danikula/AndroidVideoCache/issues .	com/kwad/sdk/core/video/cache/h.java
https://github.com/danikula/AndroidVideoCache/issues/88 .	com/kwad/sdk/core/video/cache/h.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArm64v8aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/so/exception/202305301754/ks_so-exceptionArmeabi-v7aRelease-3.3.47-e8fbb3a5f8-666.apk	com/kwad/sdk/crash/g.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac64	com/kwad/sdk/kgeo/c.java
https://p1-lm.adkwai.com/udata/pkg/KS-Android-KSAdSDK/kmac/ks_kmac32	com/kwad/sdk/kgeo/c.java
http://apps.samsung.com/appquery/appDetail.as?appId=	com/kwad/sdk/utills/d.java
https://i.snssdk.com/	com/ss/android/download/ad/api/constant/AdBaseConstants.java
https://sf6-ttcdn-tos.pstatp.com/obj/ad-tetris-site/personal-privacy-page.html	com/ss/android/download/lib/addownload/compliance/AppPrivacyPolicyActivity.java
https://apps.bytesfield.com	com/ss/android/download/lib/addownload/compliance/vc.java
https://apps.bytesfield-b.com	com/ss/android/download/lib/addownload/compliance/vc.java
https://apps.oceanengine.com/customer/api/app/pkg_info?	com/ss/android/download/lib/addownload/compliance/a.java
https://www.samsungapps.com/appquery/appDetail.as?appId=	com/ss/android/download/lib/k/m.java
https://open.weixin.qq.com/connect/sdk/qrcode/connect?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/qrcode/connect?f=json&uuiid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://zxid-m.mobileservice.cn/sdk/uaid/reportAuthToken	com/zx/a/l8b7/f1.java
https://zxid-m.mobileservice.cn/sdk/extend/tag	com/zx/a/l8b7/j1.java
https://zxid-m.mobileservice.cn/sdk/uaid/get	com/zx/a/l8b7/g1.java
https://zxid-m.mobileservice.cn/sdk/config/init	com/zx/a/l8b7/h.java
https://zxid-m.mobileservice.cn/sdk/module/getCoreModule	com/zx/a/l8b7/v.java
https://zxid-m.mobileservice.cn/sdk/channel/report	com/zx/a/l8b7/z0.java
https://zxid-m.mobileservice.cn/sdk/app/depAnalysis	com/zx/a/l8b7/r0.java
https://aid.mobileservice.cn/	com/zx/a/l8b7/q2.java

https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.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://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.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://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.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/GifTextView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
https://ask.dcloud.net.cn/article/36199	Mogua Engine V1
https://cloud.hnkzy.com/h5/	Mogua Engine V2
https://act.hnkzy.com/api/v1	Mogua Engine V2
https://act2.hnkzy.com/api/v1	Mogua Engine V2
http://dl.hnkzy.com:8081/api/v1	Mogua Engine V2
https://i.ilife798.com/api/v1	Mogua Engine V2
https://i.hnkzy.com	Mogua Engine V2
https://cloud.hnkzy.com/score/	Mogua Engine V2

https://render.alipay.com/p/h5/cloudcode-fe/redirect.html?target=	Mogua Engine V2
https://github.com/facebook/regenerator/blob/main/LICENSE	Mogua Engine V2
https://cloud.hnkzy.com/h5/	Mogua Engine V2
https://feross.org/opensource>	Mogua Engine V2
https://render.alipay.com/p/f/jfb4alj/pages/receive-redpacket/index.html?__webview_options__=ttb%253Dauto&partnerId=&sceneCode=KF_DYW02&shareChannel=QRCode&shareUserId=2088631403836084&sharedUserId=	Mogua Engine V2
http://feross.org>	Mogua Engine V2
https://netpay.cmbchina.com/netpayment/BaseHttp.dll?H5PayJsonSDK	Mogua Engine V2
https://ask.dcloud.net.cn/protocol.htm1	Mogua Engine V2
https://render.alipay.com/p/c/k2cx0tg8	Mogua Engine V2
https://wallet.95516.com/s/wl/WebAPP/helpAgree/page/agreement/regPrivacy.html?cntryCode=86	Mogua Engine V2
https://wallet.95516.com/s/wl/WebAPP/helpAgree/page/agreement/regPrivacy.html	Mogua Engine V2
http://www.cmbchina.com/personal/netbank/NetbankInfo.aspx?guid=ca085e03-b3f2-4ac8-8a35-3560e8276cb2	Mogua Engine V2
https://e.qq.com/dev/help_detail.html?cid=2005&pid=5983	Mogua Engine V2
https://www.wechat.com/zh_CN/privacy_policy.html	Mogua Engine V2
https://www.msa-alliance.cn/	Mogua Engine V2
https://privacy.oppo.com/cn/policy/	Mogua Engine V2
https://www.csjplatform.com/privacy/partner	Mogua Engine V2
https://rule.tencent.com/rule/preview/496d77fa-ee6d-4583-b16b-610fdcebbc57	Mogua Engine V2
https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050043971	Mogua Engine V2
http://partner.toutiao.com/privacy	Mogua Engine V2
https://union.baidu.com/bqt/	Mogua Engine V2
https://u.kuaishou.com/home/help/detail/1337/1220	Mogua Engine V2
https://privacy.qq.com/policy/tencent-privacypolicy	Mogua Engine V2

https://docs.getui.com/privacy	Mogua Engine V2
https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177	Mogua Engine V2
https://www.fresco-cn.org/	Mogua Engine V2
https://weexapp.com/zh/	Mogua Engine V2
https://www.thorui.cn/	Mogua Engine V2
https://ask.dcloud.net.cn/protocol.htm1	Mogua Engine V2
https://render.alipay.com/p/c/k2cx0tg8	Mogua Engine V2
https://wallet.95516.com/s/wl/WebAPP/helpAgree/page/agreement/regPrivacy.html?cntryCode=86	Mogua Engine V2
https://wallet.95516.com/s/wl/WebAPP/helpAgree/page/agreement/regPrivacy.html	Mogua Engine V2
http://www.cmbchina.com/personal/netbank/NetbankInfo.aspx?guid=ca085e03-b3f2-4ac8-8a35-3560e8276cb2	Mogua Engine V2
https://e.qq.com/dev/help_detail.html?cid=2005&pid=5983	Mogua Engine V2
https://www.wechat.com/zh_CN/privacy_policy.html	Mogua Engine V2
https://www.msa-alliance.cn/	Mogua Engine V2
https://privacy.oppo.com/cn/policy/	Mogua Engine V2
https://www.csjplatform.com/privacy/partner	Mogua Engine V2
https://rule.tencent.com/rule/preview/496d77fa-ee6d-4583-b16b-610fdcebbc57	Mogua Engine V2
https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050043971	Mogua Engine V2
http://partner.toutiao.com/privacy	Mogua Engine V2
https://union.baidu.com/bqt/	Mogua Engine V2
https://u.kuaishou.com/home/help/detail/1337/1220	Mogua Engine V2
https://privacy.qq.com/policy/tencent-privacypolicy	Mogua Engine V2
https://docs.getui.com/privacy	Mogua Engine V2
https://developer.huawei.com/consumer/cn/doc/development/HMSCore-Guides/sdk-data-security-0000001050042177	Mogua Engine V2
https://www.fresco-cn.org/	Mogua Engine V2

https://weexapp.com/zh/	Mogua Engine V2
https://service.dcloud.net.cn/uniapp/feedback.html	Mogua Engine V2
http://www.w3.org/1999/xlink	Mogua Engine V2
http://www.w3.org/2000/svg	Mogua Engine V2
http://www.w3.org/1998/Math/MathML	Mogua Engine V2
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	Mogua Engine V2
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	Mogua Engine V2
https://www.google.com/maps/?daddr=	Mogua Engine V2
https://www.google.com/maps/	Mogua Engine V2
https://quilljs.com/	Mogua Engine V2
https://quilljs.com	Mogua Engine V2

 邮箱线索

邮箱地址	所在文件
.apk@classes.dex	com/kuaishou/weapon/p0/ac.java
danikula@gmail.com	com/kwad/sdk/core/videocache/h.java
u81f3hnkzy@hnkzy.com uff1ahnkzy@hnkzy.com	Mogua Engine V2

 手机线索

 签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书

主题: C=CN, ST=hunan, L=changsha, O=hnkzy, OU=hnkzy, CN=lixiangqi
签名算法: rsassa_pkcs1v15
有效期自: 2019-05-07 01:33:14+00:00
有效期至: 2119-04-13 01:33:14+00:00
发行人: C=CN, ST=hunan, L=changsha, O=hnkzy, OU=hnkzy, CN=lixiangqi
序列号: 0xf9a4af2
哈希算法: sha256
md5值: c18d65e286321680668e33166e392358
sha1值: 726f4d617594e1a55512363d91f2a980c9445aa0
sha256值: ab264d1794220760f2f41b9b861d93dbd6e879182ceb9e87be69f2e698b69f39
sha512值: edd0f30f9bc16bf8c3c1062d315778042eb7569b30c31dcf3681b3acbc9a120a5fb5339494a665da72dfebe9a0dad8e7392e868c881aaef54bda1bf678aad17
公钥算法: rsa
密钥长度: 2048
指纹: 04506c3b55eaed71b429927698b1a6f696115837f8936d92bacfeaf8d2112220

 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_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"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"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"
"dcloud_tips_certificate" : "证书"

 加壳分析

 第三方SDK

名称	分类	URL链接
Fresco图库	开发辅助	https://reports.exodus-privacy.eu.org/trackers/468
Pangle	广告管理	https://reports.exodus-privacy.eu.org/trackers/363
fastjson	开发辅助	https://reports.exodus-privacy.eu.org/trackers/457
glide图库	开发辅助	https://reports.exodus-privacy.eu.org/trackers/469
个推	消息推送	https://reports.exodus-privacy.eu.org/trackers/460
支付宝	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/445
数字天堂（北京）网络技术有限公司	APP打包, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/444
欢太	开发辅助	https://reports.exodus-privacy.eu.org/trackers/463
移动安全联盟	设备信息	https://reports.exodus-privacy.eu.org/trackers/464
腾讯微信	身份识别, 支付平台, 开发辅助	https://reports.exodus-privacy.eu.org/trackers/447

 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.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
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.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.CAPTURE_SECURE_VIDEO_OUTPUT	正常		允许应用程序捕获安全视频输出
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.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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.BLUETOOTH_SCAN	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.cloudora.android.openadsdk.permission.TT_PANGOLIN	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.cloudora.android	未知	Unknown permission	Unknown permission from android reference
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
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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
com.hihonor.permission.MANAGE_FOLD_SCREEN	未知	Unknown permission	Unknown permission from android reference
com.hihonor.permission.MANAGE_FOLD_SCREEN_PRIVILEGED	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
	Schemes: unipush://, hnkzy://,

io.dcloud.PandoraEntry	Hosts: io.dcloud.unipush, Paths: /,
com.zhimi.cmbpay.CMBSchemeActivity	Schemes: ahffafigda://,
com.huawei.openalliance.ad.activity.PPSLauncherActivity	Schemes: hwpps://, Hosts: com.cloudora.android,