



MoGua

育托帮管理 1.1.4.APK 分析报告



APP名称:

育托帮管理

包名:

net.yutuobang.admin

域名线索:	86条
URL线索:	91条
邮箱线索:	0条
分析日期:	2025年7月3日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: net.yutuobang.admin.apk

文件大小: 33.96MB

MD5值: ac802a31dbddcd37c99b7078eba82a43

SHA1值: e28f185f62600791cdf6bd13d02f627a5f96ef97

SHA256值: 392530a6afc64613cdf5de2ba759d94625d74dc17f9600856be3f822407177f0

i APP 信息

App名称: 育托帮管理
包名: net.yutuobang.admin
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.1.4
安卓版本: 114

🔍 域名线索

域名	服务器信息
www.google.com	IP: 199.16.158.9 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
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
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
	IP: 49.4.45.231 所属国家: China

grs.dbankcloud.cn	地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
cgicol.amap.com	IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
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
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
wap.amap.com	IP: 175.22.51.222 所属国家: China 地区: Jilin 城市: Changchun 纬度: 43.880001 经度: 125.322777
d-gt.getui.com	没有服务器地理信息.
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

cdn.yutuobang.net	IP: 101.28.133.74 所属国家: China 地区: Hebei 城市: Handan 纬度: 36.600559 经度: 114.467781
lame.sf.net	IP: 104.18.20.237 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
sdk-open-phone.getui.com	IP: 101.68.218.174 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
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
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
lbs.amap.com	IP: 110.253.188.148 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349

er.dcloud.io	没有服务器地理信息.
b-gtc.getui.nethttps	没有服务器地理信息.
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
utils.yutuobang.net	IP: 121.40.163.230 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
mps.amap.com	IP: 203.119.169.143 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
	IP: 140.207.191.167 所属国家: China

mp.weixin.qq.com	地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
grs.platform.dbankcloud.ru	没有服务器地理信息.
play.google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
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
stream.mobihhtml5.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
gtc.getui.nethttps	没有服务器地理信息.
maps.testing.amap.com	IP: 59.82.57.204 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 110.253.189.212 所属国家: China

wb.amap.com	地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
mdc.html5.qq.com	IP: 116.130.223.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tbsrecovery.imtt.qq.com	IP: 61.181.204.91 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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
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
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
	IP: 116.128.171.214 所属国家: China

open.weixin.qq.com	地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
quilljs.com	IP: 172.66.40.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mpsapi.amap.com	IP: 203.119.169.143 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
restsdk.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
data.yutuobang.net	IP: 101.67.62.25 所属国家: China 地区: Zhejiang 城市: Huzhou 纬度: 30.870550 经度: 120.093300
resolver.msg.xiaomi.net	IP: 110.43.0.169 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 80.158.49.244 所属国家: Germany

data-dre.push.dbankcloud.com	地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
yuntuapi.amap.com	没有服务器地理信息.
apiinit.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
m3w.cn	IP: 221.204.14.200 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
cn.register.xmpush.xiaomi.com	IP: 221.194.179.52 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
grs.dbankcloud.eu	没有服务器地理信息.
apis.map.qq.com	IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.com	IP: 60.28.200.159 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181

	经度: 117.176102
cfg.imtt.qq.com	IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
crbug.com	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
er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
stream.dcloud.net.cn	IP: 43.142.166.20 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ask.dcloud.net.cn	IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dualstack-a.apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing

	纬度: 39.907501 经度: 116.397102
upload.yutuobang.net	IP: 101.67.62.33 所属国家: China 地区: Zhejiang 城市: Huzhou 纬度: 30.870550 经度: 120.093300
wprd0d.is.autonavi.com	没有服务器地理信息.
m5.amap.com	IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
data-drcn.push.dbankcloud.com	IP: 121.36.117.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 159.138.203.215

metrics5.dt.dbankcloud.ru	所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg 纬度: 56.857498 经度: 60.612499
log.tbs.qq.com	IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
shop.yutuobang.net	IP: 116.142.237.86 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
xml.org	IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest 纬度: 29.499678 经度: -98.399246
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.asia	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572

schemas.android.com	没有服务器地理信息.
api.yutuobang.net	IP: 121.41.83.136 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
appgallery.cloud.huawei.com	IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
c-gtc.getui.nethttps	没有服务器地理信息.
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
tbs.imtt.qq.com	IP: 61.161.0.179 所属国家: China 地区: Jilin 城市: Siping 纬度: 43.163330 经度: 124.368607
norma-external-collect.meizu.com	没有服务器地理信息.

at.alicdn.com	IP: 221.195.63.238 所属国家: China 地区: Hebei 城市: Cangzhou 纬度: 38.316669 经度: 116.866669
ns.adobe.com	没有服务器地理信息.
page.yutuobang.net	IP: 101.28.133.122 所属国家: China 地区: Hebei 城市: Handan 纬度: 36.600559 经度: 114.467781
adiu.amap.com	IP: 110.253.189.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
admin.yutuobang.net	IP: 47.97.97.182 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
dualstack-arestapi.amap.com	IP: 203.119.169.174 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650

	经度: 120.161583
mst01.is.autonavi.com	IP: 110.253.188.147 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
metrics-dra.dt.hicloud.com	IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281

URL线索

URL信息	Url所在文件
https://adiu.amap.com/ws/device/adius	com/amap/api/col/p0003l/hk.java
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&	com/amap/api/col/p0003l/je.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/p0003l/fh.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/p0003l/fh.java
https://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003l/gu.java
http://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/p0003l/gu.java
http://restsdk.amap.com/v3/place/text?	com/amap/api/col/p0003l/a.java
http://restsdk.amap.com/v3/place/around?	com/amap/api/col/p0003l/a.java

http://restsdk.amap.com/v3/config/district?	com/amap/api/col/p0003l/a.java
http://restsdk.amap.com	com/amap/api/col/p0003l/fq.java
http://restsdk.amap.com/v4/grasproad/driving?	com/amap/api/col/p0003l/fb.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003l/df.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003l/s.java
http://wprd0%d.is.autonavi.com/appmaptile?	com/amap/api/col/p0003l/de.java
http://restsdk.amap.com/v4/gridmap?	com/amap/api/col/p0003l/de.java
http://restsdk.amap.com/v4	com/amap/api/col/p0003l/cr.java
http://restsdk.amap.com	com/amap/api/col/p0003l/v.java
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\	com/amap/api/col/p0003l/l.java
https://adiu.amap.com/ws/device/adius	com/amap/api/col/s/df.java
http://apiinit.amap.com/v3/log/init	com/amap/api/col/s/bt.java
http://restsdk.amap.com/v3	com/amap/api/col/s/i.java
https://restsdk.amap.com/v3	com/amap/api/col/s/i.java
http://restsdk.amap.com/v4	com/amap/api/col/s/i.java
https://restsdk.amap.com/v4	com/amap/api/col/s/i.java
http://restsdk.amap.com/v5	com/amap/api/col/s/i.java
https://restsdk.amap.com/v5	com/amap/api/col/s/i.java
http://yuntuapi.amap.com	com/amap/api/col/s/i.java

https://yuntuapi.amap.com	com/amap/api/col/s/i.java
http://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/s/i.java
https://restsdk.amap.com/rest/me/cpoint	com/amap/api/col/s/i.java
http://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/s/i.java
https://m5.amap.com/ws/mapapi/shortaddress/transform	com/amap/api/col/s/i.java
https://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/s/cu.java
http://restsdk.amap.com/sdk/compliance/params	com/amap/api/col/s/cu.java
https://restsdk.amap.com/v3/iasdkauth	com/amap/api/col/s/bs.java
https://dualstack-arestapi.amap.com/v3/iasdkauth	com/amap/api/col/s/bs.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/bo.java
http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0	com/amap/api/col/s/bo.java
http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0	com/amap/api/col/s/bo.java
http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0	com/amap/api/col/s/bo.java
http://wap.amap.com/	com/amap/api/maps/AMapUtils.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/	com/amap/api/location/AMapLocation.java
http://apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utls/b.java
http://dualstack-a.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utls/b.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utls/b.java

http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/utils/g.java
http://abroad.apilocate.amap.com/mobile/binary	com/autonavi/aps/amapapi/trans/a.java
http://dualstack-arestapi.amap.com/v3/geocode/regeo	com/autonavi/aps/amapapi/trans/c.java
http://restsdk.amap.com/v3/geocode/regeo	com/autonavi/aps/amapapi/trans/c.java
http://restsdk.amap.com/rest/lbs/dem/data?z=%d&x=%d&y=%d&type=2	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mst01.is.autonavi.com/appmaptile? z=%d&x=%d&y=%d&lang=zh_cn&size=1&scale=1&style=6	com/autonavi/base/ae/gmap/TerrainOverlayProvider.java
http://mpsapi.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/ae/gmap/GLMapEngine.java
http://m5.amap.com/	com/autonavi/base/amap/mapcore/maploader/AMapLoader.java
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
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
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/XmlPullParserFactorySecurity.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
http://bi.	com/igexin/push/config/b.java
http://config.	com/igexin/push/config/b.java
http://bi.	com/igexin/push/config/g.java
http://config.	com/igexin/push/config/g.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
https://api-push.meizu.com/garcia/api/client/log/upload	com/meizu/cloud/pushsdk/platform/a/a.java
https://api-push.meizu.com/garcia/api/server/getPublicKey	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://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/qrcodeconnect?appid=%s&noncestr=%s×tamp=%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=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://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://log.tbs.qq.com/ajax?c=pu&v=2&k=	com.tencent.smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=pu&tk=	com.tencent.smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=dl&k=	com.tencent.smtt/utls/o.java
https://cfg.imtt.qq.com/tbs?v=2&mk=	com.tencent.smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=ul&v=2&k=	com.tencent.smtt/utls/o.java
https://mqqqad.html5.qq.com/adjs	com.tencent.smtt/utls/o.java
https://log.tbs.qq.com/ajax?c=ucfu&k=	com.tencent.smtt/utls/o.java
https://tbsrecovery.imtt.qq.com/getconfig	com.tencent.smtt/utls/o.java
https://tbs.imtt.qq.com/plugin/DebugPlugin_v2.tbs	com.tencent.smtt/utls/d.java

http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fa.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fs.java
https://%1\$s/gslb?ver=5.0	com/xiaomi/push/bt.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/ft.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/en.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/az.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/cp.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
http://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://stream.mobih5.com/	io/dcloud/common/constant/StringConst.java
https://stream.dcloud.net.cn/	io/dcloud/common/constant/StringConst.java
http://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.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://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/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/b.java
https://er.dcloud.net.cn/rv	io/dcloud/e/c/h/b.java
http://lbs.amap.com/api/android-sdk/guide/error/	io/dcloud/js/map/amap/adapters/AMapLink.java
http://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://play.google.com/store/apps/details?id=	摸瓜V1引擎
https://appgallery.cloud.huawei.com	摸瓜V1引擎
https://metrics1.data.hicloud.com:6447	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://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://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://page.yutuobang.net/defaults/user-usage-protocol.html\	摸瓜V2引擎
https://page.yutuobang.net/defaults/user-privacy-protocol.html\	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://cdn.yutuobang.net/defaults/wx-mp-empty.html	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://page.yutuobang.net/defaults/user-	摸瓜V2引擎
">https://feross.org/opensource>	摸瓜V2引擎

http://feross.org>	摸瓜V2引擎
https://data.yutuobang.net	摸瓜V2引擎
https://cdn.yutuobang.net	摸瓜V2引擎
https://admin.yutuobang.net	摸瓜V2引擎
https://shop.yutuobang.net	摸瓜V2引擎
https://api.yutuobang.net	摸瓜V2引擎
https://upload.yutuobang.net	摸瓜V2引擎
https://utils.yutuobang.net	摸瓜V2引擎
https://page.yutuobang.net/prod	摸瓜V2引擎
https://cdn.yutuobang.net/defaults/jz_insurance.jpg_thumb200	摸瓜V2引擎
https://cdn.yutuobang.net/defaults/jz_health.jpg_thumb200	摸瓜V2引擎
https://mp.weixin.qq.com/s?__biz=MzUzMtAwODA2MA==&mid=2247484243&idx=1&sn=dbfa4ac89949a84d94511798f6d6f8fb	摸瓜V2引擎
https://page.yutuobang.net/defaults/user-usage-protocol.html?v	摸瓜V2引擎
https://page.yutuobang.net/defaults/user-privacy-protocol.html?v	摸瓜V2引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf)	摸瓜V2引擎
https://cdn.yutuobang.net/defaults/admin-menus-fonts/iconfont.ttf)	摸瓜V2引擎

https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://cdn.yutuobang.net/defaults/wx-mp-empty.html	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://crbug.com/v8/8520	lib/armeabi-v7a/libweexjss.so
http://lame.sf.net	lib/armeabi-v7a/liblamemp3.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-image-transcoder.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libstatic-webp.so
http://mpsapi.amap.com/ws/mps/vmap/	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/rtt/	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/smap	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/rtt	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/vmap	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so

https://mps.amap.com/ws/mps/smap	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/spot	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/hot	lib/armeabi-v7a/libAMapSDK_MAP_v9_5_0.so
https://crbug.com/v8/8520	lib/arm64-v8a/libweexjss.so
http://lame.sf.net	lib/arm64-v8a/liblamemp3.so
http://mpsapi.amap.com/ws/mps/vmap/	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/rtt/	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://mpsapi.amap.com/	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
http://m5.amap.com	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/rtt	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/vmap	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/spot	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so
https://mps.amap.com/ws/mps/hot	lib/arm64-v8a/libAMapSDK_MAP_v9_5_0.so

邮箱线索

手机线索

手机号	所在文件
14222222222	com/amap/api/col/s/bs.java
18222222222	com/tencent/smtt/sdk/o.java

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=, L=, O=Android, OU=Android, CN=%2FL0tnlZk5JqH%2BbXNPh3PHFcUN5QJqpXFskw4deE6E5FoqRAmqPZ12%2B4HeWfKD6%2FUfPVzrn%2FuHKPIbLdhAIG3Hg%3D%3D
签名算法: rsassa_pkcs1v15
有效期自: 2023-03-21 08:42:06+00:00
有效期至: 2123-02-25 08:42:06+00:00
发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=%2FL0tnlZk5JqH%2BbXNPh3PHFcUN5QJqpXFskw4deE6E5FoqRAmqPZ12%2B4HeWfKD6%2FUfPVzrn%2FuHKPIbLdhAIG3Hg%3D%3D
序列号: 0x3226940
哈希算法: sha256
md5值: 06e707564905e3c66092091bdfd58704
sha1值: 9182604d36b8ff3247df851cc22a28d2c938d9c5
sha256值: 36467198ad30c05e33b38ce6be1c4bb1a7189a973f2a48a530646d454aea02a2
sha512值: 7864e46ab0d0e7e4a6b494840c8a54e694328e80c5f6178dc8ff352c5fe2c46eefeb9bb35afa53e2122248d6287d2b0a50b8dac9453b803db949d06bd0d9f729
公钥算法: rsa
密钥长度: 2048
指纹: cf2f0098b92b44e4ca2a2e2be2ff1fdd0b49024b9be329429347927111c25b33

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"
"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

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
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.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.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_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.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
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.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.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.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

net.yutuobang.admin.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
net.yutuobang.admin.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
getui.permission.GetuiService.net.yutuobang.admin	未知	Unknown permission	Unknown permission from android reference
net.yutuobang.admin.permission.MIPUSH_RECEIVE	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
com.vivo.notification.permission.BADGE_ICON	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
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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.meizu.flyme.permission.PUSH	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
net.yutuobang.admin.permission.PROCESS_PUSH_MSG	未知	Unknown	Unknown permission from android reference

		permission	
net.yutuobang.admin.permission.PUSH_PROVIDER	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://, ytbadmin://, Hosts: io.dcloud.unipush, Paths: /,