MoGua

APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成

相亲站 3.7.6.APK

APP名称:	相亲站
包名:	cn.xiangqinzhan
域名线索:	63条
URL线索:	90条
邮箱线索:	0条
分析日期:	2022年1月28日 23:20

文件信息

文件名: xiangqinzhan161794.apk
文件大小: 11.85MB
MD5值: 89b02bde387261ac7817a4c6e519043c
SHA1值: 840b4b5a403d3a74a671e46b9ee71ea7896d16a9
SHA256值: 78e936934598ea6416a7150778a53e37e76e641fbbe63596e830d898353c9c34

APP 信息

App名称: 相亲站
包名: cn.xiangqinzhan
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 3.7.6
安卓版本: 376

域名线索

域名	是否危险域名	服务器信息
mapoffdownload.bdstatic.com	good	**IP:** 218.68.136.36 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
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

域名	是否危险域名	服务器信息
mobilegw.aaa.alipay.net	good	没有服务器地理信息.
wapmap.baidu.com	good	**IP:** 111.206.209.212 **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
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
loc.map.baidu.com	good	**IP:** 111.206.209.175 **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
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

域名	是否危险域名	服务器信息
register.xmpush.global.xiaomi.com	good	**IP:** 47.88.199.5 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
cp01-lbs-api01.cp01.baidu.com	good	没有服务器地理信息.
loggw-exsdk.alipay.com	good	**IP:** 110.75.130.122 **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.
c-hzgt2.getui.com	good	**IP:** 183.131.7.106 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

域名	是否危险域名	服务器信息
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
www.baidu.com	good	**IP:** 110.242.68.3 **所属国家:** China **地区:** Hebei **城市:** Baoding **纬度:** 38.851109 **经度:** 115.490280 **查看地图:** Google Map
cn.register.xmpush.xiaomi.com	good	**IP:** 118.26.252.220 **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
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

域名	是否危险域名	服务器信息
daup.map.baidu.com	good	**IP:** 153.3.236.86 **所属国家:** China **地区:** Jiangsu **城市:** Nanjing **纬度:** 32.061668 **经度:** 118.777779 **查看地图:** Google Map
j.map.baidu.com	good	**IP:** 111.206.209.187 **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
api.map.baidu.com	good	**IP:** 111.206.209.166 **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.stable.alipay.net	good	没有服务器地理信息.
v.map.baidu.com	good	**IP:** 111.206.209.185 **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
bbs.lbsyun.baidu.com	good	**IP:** 111.206.208.72 **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
resolver.msg.xiaomi.net	good	**IP:** 183.84.5.221 **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
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
store.hispace.hicloud.com	good	**IP:** 49.4.18.123 **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
vectormap0.bdimg.com	good	**IP:** 61.156.44.35 **所属国家:** China **地区:** Shandong **城市:** Laiwu **纬度:** 36.192780 **经度:** 117.656937 **查看地图:** Google Map
resolver.msg.global.xiaomi.net	good	**IP:** 47.241.174.254 **所属国家:** Singapore **地区:** Singapore **城市:** Singapore **纬度:** 1.289670 **经度:** 103.850067 **查看地图:** Google Map
api-push.in.meizu.com	good	**IP:** 206.161.233.191 **所属国家:** United States of America **地区:** Virginia **城市:** Herndon **纬度:** 38.978210 **经度:** -77.386993 **查看地图:** Google Map
idmb.register.xmpush.global.xiaomi.com	good	**IP:** 15.206.99.29 **所属国家:** India **地区:** Maharashtra **城市:** Mumbai **纬度:** 19.014410 **经度:** 72.847939 **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
newclient.map.baidu.com	good	**IP:** 111.206.209.170 **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
www.xiangqinzhan.cn	good	**IP:** 101.200.185.196 **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
www.jivesoftware.com	good	**IP:** 35.238.7.255 **所属国家:** United States of America **地区:** Iowa **城市:** Council Bluffs **纬度:** 41.261940 **经度:** -95.860832 **查看地图:** Google Map

域名	是否危险域名	服务器信息
api-push.meizu.com	good	**IP:** 125.94.213.129 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
xmlpull.org	good	**IP:** 74.50.61.58 **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
app.navi.baidu.com	good	**IP:** 111.206.209.213 **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
m.alipay.com	good	**IP:** 203.209.245.120 **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
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
xml.org	good	**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 **查看地图:** Google Map
itsdata.map.baidu.com	good	**IP:** 111.206.209.180 **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
map.baidu.com	good	**IP:** 111.206.208.32 **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
play.google.com	good	**IP:** 172.217.160.110 **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

域名	是否危险域名	服务器信息
ru.register.xmpush.global.xiaomi.com	good	IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752220 经度: 37.615559 查看地图: Google Map
sv.map.baidu.com	good	IP: 111.206.209.186 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
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
mclient.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

域名	是否危险域名	服务器信息
appgallery.cloud.huawei.com	good	**IP:** 117.78.15.51 **所属国家:** China **地区:** Guangdong **城市:** Guangzhou **纬度:** 23.116671 **经度:** 113.250000 **查看地图:** Google Map
offmap2.baidu.com	good	**IP:** 220.194.65.35 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
mobilegw-1-64.test.alipay.net	good	没有服务器地理信息.
mobilegw.alipay.com	good	**IP:** 203.209.245.78 **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
sdk.open.phone.igexin.com	good	**IP:** 124.160.127.216 **所属国家:** China **地区:** Zhejiang **城市:** Hangzhou **纬度:** 30.293650 **经度:** 120.161423 **查看地图:** Google Map

域名	是否危险域名	服务器信息
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
m3w.cn	good	**IP:** 125.37.206.223 **所属国家:** China **地区:** Tianjin **城市:** Tianjin **纬度:** 39.142220 **经度:** 117.176666 **查看地图:** Google Map
itsmap3.baidu.com	good	**IP:** 153.37.235.49 **所属国家:** China **地区:** Jiangsu **城市:** Suzhou **纬度:** 31.311390 **经度:** 120.618057 **查看地图:** Google Map
d-gt.getui.com	good	没有服务器地理信息.
indoorsearch.map.baidu.com	good	**IP:** 111.206.209.201 **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
norma-external-collect.meizu.com	good	IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan 纬度: 22.520580 经度: 113.382317 查看地图: Google Map
render.alipay.com	good	IP: 42.81.213.243 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
daohang.map.baidu.com	good	IP: 111.206.209.190 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
client.map.baidu.com	good	IP: 111.206.209.119 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map

域名	是否危险域名	服务器信息
fr.register.xmpush.global.xiaomi.com	good	**IP:** 18.185.221.188 **所属国家:** Germany **地区:** Hessen **城市:** Frankfurt am Main **纬度:** 50.115520 **经度:** 8.684170 **查看地图:** Google Map
newvector.map.baidu.com	good	**IP:** 111.206.209.171 **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
h5.m.taobao.com	good	**IP:** 140.249.89.233 **所属国家:** China **地区:** Shandong **城市:** Jinan **纬度:** 36.668331 **经度:** 116.997223 **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

URL信息	Url所在文件
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/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

URL信息	Url所在文件
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
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
https://api.map.baidu.com/sdkproxy/lbs_navsdk_mini/tripshare/v1/trip/search	com/baidu/mapsdkplatform/comapi/synchronization/b/g.java
http://cp01-lbs-api01.cp01.baidu.com:8108/lbs_navsdk_mini/tripshare/v1/trip/search	com/baidu/mapsdkplatform/comapi/synchronization/b/g.java
https://api.map.baidu.com/sdkproxy/lbs_android/tripshare/v1/passenger/pullpath	com/baidu/mapsdkplatform/comapi/synchronization/c/f.java
http://api.map.baidu.com/sdkproxy/lbs_android/tripshare/v1/passenger/pullpath	com/baidu/mapsdkplatform/comapi/synchronization/c/f.java
https://api.map.baidu.com/lbs_sdkcc/report	com/baidu/mapsdkplatform/comapi/b/a/c.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/custom/v2/getjsonstyle	com/baidu/mapsdkplatform/comapi/util/CustomMapStyleLoader.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/custom/v2/getjsonstyle	com/baidu/mapsdkplatform/comapi/util/CustomMapStyleLoader.java
http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461	com/baidu/mapsdkplatform/comapi/util/PermissionCheck.java

URL信息	Url所在文件
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/search	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/detail	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/indoor/v1/	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/suggestion	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/geocoder/v2	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/transit	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui2/v1/	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/riding	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui/v1/	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/	com/baidu/platform/domain/b.java
https://j.map.baidu.com/	com/baidu/platform/domain/b.java
https://client.map.baidu.com/imap/share/ps	com/baidu/platform/domain/b.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/s	com/baidu/platform/domain/b.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/search	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/detail	com/baidu/platform/domain/a.java

URL信息	Url所在文件
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/indoor/v1/	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/place/v2/suggestion	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/v2/lbs_androidsdk/geocoder/v2	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/transit	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui2/v1/	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/pathplan/v2/riding	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/phpui/v1/	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/	com/baidu/platform/domain/a.java
http://j.map.baidu.com/	com/baidu/platform/domain/a.java
http://client.map.baidu.com/imap/share/ps	com/baidu/platform/domain/a.java
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/apimap/v1/s	com/baidu/platform/domain/a.java
http://map.baidu.com/?newmap=1&s=	com/baidu/platform/core/e/e.java
http://wapmap.baidu.com/s?tn=Detail&pid=	com/baidu/platform/core/e/c.java
http://itsdata.map.baidu.com/long-conn-gps/sdk.php	com/baidu/location/a/f.java
http://loc.map.baidu.com/cc.php	com/baidu/location/a/d.java

URL信息	Url所在文件
http://loc.map.baidu.com/oqur.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/tcu.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/rtbu.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/iofd.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/wloc	com/baidu/location/d/k.java
http://loc.map.baidu.com/sdk.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/user_err.php	com/baidu/location/d/k.java
http://loc.map.baidu.com/sdk_ep.php	com/baidu/location/d/k.java
https://loc.map.baidu.com/sdk.php	com/baidu/location/d/k.java
https://daup.map.baidu.com/cltr/rcvr	com/baidu/location/d/k.java
https://api.map.baidu.com/geosearch/v2/bound	com/baidu/mapapi/cloud/BoundSearchInfo.java
http://api.map.baidu.com/geosearch/v2/bound	com/baidu/mapapi/cloud/BoundSearchInfo.java
https://api.map.baidu.com/geosearch/v2/local	com/baidu/mapapi/cloud/LocalSearchInfo.java
http://api.map.baidu.com/geosearch/v2/local	com/baidu/mapapi/cloud/LocalSearchInfo.java
https://api.map.baidu.com/sdkproxy/lbs_androidsdk/cloudrgc/v1	com/baidu/mapapi/cloud/CloudRgcInfo.java

URL信息	Url所在文件
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/cloudrgc/v1	com/baidu/mapapi/cloud/CloudRgcInfo.java
https://api.map.baidu.com/geosearch/v2/detail/	com/baidu/mapapi/cloud/DetailSearchInfo.java
http://api.map.baidu.com/geosearch/v2/detail/	com/baidu/mapapi/cloud/DetailSearchInfo.java
https://api.map.baidu.com/geosearch/v2/nearby	com/baidu/mapapi/cloud/NearbySearchInfo.java
http://api.map.baidu.com/geosearch/v2/nearby	com/baidu/mapapi/cloud/NearbySearchInfo.java
http://app.navi.baidu.com/mobile/#navi/naving/	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/#navi/naving/start=	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://daohang.map.baidu.com/mobile/#search/search/qt=nav&sn=2$$$$$$	com/baidu/mapapi/navi/BaiduMapNavigation.java
http://map.baidu.com/zt/client/index/?fr=sdk_	com/baidu/mapapi/utils/OpenClientUtil.java
http://api.map.baidu.com/place/detail?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/place/search?	com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java
http://api.map.baidu.com/direction?	com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java
https://api.map.baidu.com/sdkcs/verify	com/baidu/lbsapi/auth/LBSAuthManager.java
https://sdk.open.phone.igexin.com/api.php	com/igexin/push/a.java
https://c-hzgt2.getui.com/api.php	com/igexin/push/a.java

URL信息	Url所在文件
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
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
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

URL信息	Url所在文件
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#process-namespaces	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#report-namespace-prefixes	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#process-docdecl	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#validation	com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fp.java
https://%1$s/gslb/?ver=4.0	com/xiaomi/push/bu.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gi.java

URL信息	Url所在文件
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/gj.java
http://xmlpull.org/v1/doc/features.html#process-namespaces	com/xiaomi/push/fd.java
http://www.jivesoftware.com/xmlns/xmpp/properties	com/xiaomi/push/gb.java
https://resolver.msg.global.xiaomi.net/psc/?t=a	com/xiaomi/push/service/aw.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/aw.java
www.baidu.com:80	com/xiaomi/push/service/r.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/cm.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/cm.java
https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/cm.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/cm.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/cm.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

URL信息	Url所在文件
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/splash-screen/report	io/dcloud/feature/gg/dcloud/ADHandler.java
http://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://ask.dcloud.net.cn/article/29	io/dcloud/js/map/adapter/DHMapView.java
http://ask.dcloud.net.cn/article/285	io/dcloud/js/map/adapter/BaiduErrorLink.java
http://ask.dcloud.net.cn/article/283	io/dcloud/i/b.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://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s	io/dcloud/g/b/c.java
https://96f0e031-f37a-48ef-84c7-2023f6360c0a.bspapp.com/http/rewarded-video/report?p=a&t=	io/dcloud/g/b/h/a.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/35877	io/dcloud/g/a/a.java
https://ask.dcloud.net.cn/article/36199	Android String Resource
http://ask.dcloud.net.cn/article/29	Android String Resource

URL信息	Url所在文件
http://www.xiangqinzhan.cn/role.html	Android String Resource
http://www.xiangqinzhan.cn/pro.html	Android String Resource
https://play.google.com/store/apps/details?id=	Android String Resource
https://appgallery.cloud.huawei.com	Android String Resource
https://store.hispace.hicloud.com/hwmarket/api/	Android String Resource
http://client.map.baidu.com/imap/sdk/tj?qt=vmap	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
http://api.map.baidu.com/sdkproxy/lbs_androidsdk/statistics/v1/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newclient.map.baidu.com/client/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://client.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://v.map.baidu.com/low/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://v.map.baidu.com/indoorinside/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://v.map.baidu.com/high/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newclient.map.baidu.com/pic/newvector/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newvector.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://vectormap0.bdimg.com/vecdata/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so

URL信息	Url所在文件
https://newclient.map.baidu.com/its/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://itsmap3.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newvector.map.baidu.com/starpic/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
http://api.map.baidu.com/sdkws/heatmap?	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://sv.map.baidu.com	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://sv.map.baidu.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://client.map.baidu.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://offmap2.baidu.com/offline-search/?	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://mapoffdownload.bdstatic.com/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newvector.map.baidu.com/grid_vc/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newvector.map.baidu.com/travel_vc/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://newvector.map.baidu.com/inst_grid/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
https://indoorsearch.map.baidu.com/is/	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.so
http://client.map.baidu.com/?qt=rg&mmproxyver=1&url=	lib/armeabi-v7a/libBaiduMapSDK_map_v5_4_1.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

向手机申请的权限	是否危险	类型	详细情况
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

向手机申请的权限	是否危险	类型	详细情况
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.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.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

向手机申请的权限	是否危险	类型	详细情况
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
getui.permission.GetuiService.cn.xiangqinzhan	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	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
cn.xiangqinzhan.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
cn.xiangqinzhan.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference

向手机申请的权限	是否危险	类型	详细情况
cn.xiangqinzhan.permission.MIPUSH_RECEIVE	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
cn.xiangqinzhan.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
cn.xiangqinzhan.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	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: C=86, ST=北京, L=海淀, O=数字天堂（北京）网络技术有限公司, OU=数字天堂（北京）网络技术有限公司, CN=DH
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2013-04-22 06:45:31+00:00
Valid To: 3012-08-23 06:45:31+00:00
Issuer: C=86, ST=北京, L=海淀, O=数字天堂（北京）网络技术有限公司, OU=数字天堂（北京）网络技术有限公司, CN=DH
Serial Number: 0x5174dc8b
Hash Algorithm: sha1
md5: 59201cf6589202cb2cdab26752472112
sha1: baad093a82829fb432a7b28cb4ccf0e9f37dae58
sha256: d75c1fa2b9ae867ce688a8adc6deac7cd6ba96f43a751fd10a200fa5974ac636
sha512: 16a37ece684bec4a3608fd375cd189eecd78eb7163a3afd1654225148e71ae07cce7755c0a9e8466dd4be505d526c19f7340a2040bd3f43004081ea409f70146
PublicKey Algorithm: rsa
Bit Size: 1024
Fingerprint: 426f7db3074401182137b947e553230a7e4c1801f824985f9fce57d65753f781

Exodus威胁情报

名称	分类	URL链接
Baidu Location		https://reports.exodus-privacy.eu.org/trackers/97
Baidu Map		https://reports.exodus-privacy.eu.org/trackers/99
Huawei Mobile Services (HMS) Core	Analytics, Advertisement, Location	https://reports.exodus-privacy.eu.org/trackers/333

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"

可能的敏感信息
"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_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"

应用内通信

活动(ACTIVITY)	通信(INTENT)
io.dcloud.PandoraEntry	Schemes: h5d24074b://,

加壳分析

文件列表	分析结果
classes.dex	壳列表 / 详细情况 反虚拟机：Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.PRODUCT check Build.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 编译器：r8

<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>

报告由 摸瓜平台 自动生成，并非包含所有检测结果，有疑问请联系管理员。

查诈骗APP | 查木马APP | 违法APP分析 | APK代码分析