



天天娱乐 99.9.3.APK 分析报告



APP名称:

天天娱乐

包名: com.taobei.sandaier

域名线索: 82条

URL线索: 77条

邮箱线索: 1条

分析日期: 2024年4月24日

分析平台: [摸瓜反编译平台](#)

文件名: o_1gcbpeqdh1b1qq0ubl15664cea (1).apk
文件大小: 15.65MB
MD5值: 429f35fde883455ee18f9290783fa72a
SHA1值: ee48088b7df9b34983d60d62ceff002e43bc04d1
SHA256值: 863e4a7b16d687f08ea6ce8e537ae15dfe3ec981b353fbf075130e313aa58736

i APP 信息

App名称: 天天娱乐
包名: com.taobei.sandaier
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 99.9.3
安卓版本: 9993

🔍 域名线索

域名	服务器信息
example.com	IP: 93.184.216.34 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.043720 经度: -77.487488
tsis.jpush.cn	IP: 183.232.58.228 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.116671 经度: 113.250000
botserverh5.aiwaya.cn	IP: 62.192.191.35 所属国家: Hong Kong 地区: Hong Kong

	城市: Hong Kong 纬度: 22.285521 经度: 114.157692
rqd.uu.qq.com	IP: 175.27.12.121 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
mobilegw.aaa.alipay.net	没有服务器地理信息.
ulogs.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
wappaygw.alipay.com	IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
apilocate.amap.com	IP: 106.11.43.81 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
wxqas.yayaim.com	IP: 107.148.240.197 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.333698 经度: -121.889297

c.isdspeed.qq.com	没有服务器地理信息.
data.iapppay.com	IP: 161.123.92.121 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.714272 经度: -74.005966
xiangliao.kaicd.com	IP: 3.18.7.81 所属国家: United States of America 地区: Ohio 城市: Columbus 纬度: 39.961182 经度: -82.998787
cgi.connect.qq.com	IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
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: 120.161423
cfg.imtt.qq.com	IP: 175.27.12.246 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 106.11.43.81

apilocatesrc.amap.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
cgicol.amap.com	IP: 59.82.60.46 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
thirdwx.qlogo.cn	IP: 175.27.38.196 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
api.weixin.qq.com	IP: 81.69.216.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
appsupport.qq.com	IP: 175.27.9.14 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
upfile.aiwaya.cn	IP: 62.192.191.35 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
debugx5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
huatuocode.huatuo.qq.com	没有服务器地理信息.
city.ip138.com	没有服务器地理信息.
lbs.amap.com	IP: 59.82.31.149 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
plbslog.umeng.com	IP: 36.156.202.73 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ip.taobao.com	IP: 59.82.31.182 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.apple.com	IP: 27.148.139.136 所属国家: China 地区: Fujian 城市: Fuzhou 纬度: 26.061390

	经度: 119.306107
long.open.weixin.qq.com	IP: 109.244.216.15 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
soft.tbs.imtt.qq.com	IP: 121.51.175.60 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
mcgw.alipay.com	IP: 124.239.239.237 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
mclient.alipay.com	IP: 124.239.239.236 所属国家: China 地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
wspeed.qq.com	没有服务器地理信息.

mobilegw.alipay.com	IP: 203.209.250.2 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
188.188.1.94	IP: 188.188.1.94 所属国家: Belgium 地区: Hainaut 城市: Charleroi 纬度: 50.411362 经度: 4.444480
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
alogsus.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
log.tbs.qq.com	IP: 109.244.244.37 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
voice.aiwaya.cn	IP: 62.192.191.35 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521

	经度: 114.157692
m.alipay.com	IP: 203.209.245.74 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
lark.alipay.com	IP: 119.42.230.126 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
payment.iapppay.com	IP: 161.123.92.121 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.714272 经度: -74.005966
cdn.jtcfgames.com	没有服务器地理信息.
abroad.apilocate.amap.com	IP: 59.82.44.11 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
lame.sf.net	IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego 纬度: 32.799797 经度: -117.137047

mobilegw-1-64.test.alipay.net	没有服务器地理信息.
wup.imtt.qq.com	IP: 182.254.57.56 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
182.92.20.189	IP: 182.92.20.189 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
fusion.qq.com	IP: 121.51.36.15 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
ssgw.updrips.com	没有服务器地理信息.
mobilegw.stable.alipay.net	没有服务器地理信息.
120.24.210.161	IP: 120.24.210.161 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
h5.m.taobao.com	IP: 220.181.135.233 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501

	经度: 116.397232
developer.umeng.com	IP: 59.82.29.163 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
open.weixin.qq.com	IP: 109.244.144.48 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ulogs.umengcloud.com	IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
upfile.hqsuntek.com	IP: 8.140.184.129 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
pms.mb.qq.com	IP: 109.244.173.227 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 47.246.110.94 所属国家: Hong Kong

ouplog.umeng.com	地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
cmnsguider.yunos.com	IP: 203.119.169.83 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
restapi.amap.com	IP: 203.119.175.194 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
openmobile.qq.com	IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ipay.iapppay.com	IP: 161.123.92.121 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.714272 经度: -74.005966
iapppay-data.iapppay.com	IP: 161.123.92.121 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.714272 经度: -74.005966

android.bugly.qq.com	IP: 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
117.50.17.160	IP: 117.50.17.160 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.222219 经度: 121.458061
alogus.umeng.com	IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
qzs.qq.com	IP: 182.254.54.197 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
119.29.29.29	IP: 119.29.29.29 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
xmlpull.org	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
debugtbs.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.qq.com	IP: 175.27.8.138 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
paygate-yf.meituan.com	IP: 101.236.12.31 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
www.openssl.org	IP: 184.27.21.43 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
mdc.html5.qq.com	IP: 175.27.9.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 203.119.144.20 所属国家: China

hydra.alibaba.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
iapppay.halodigit.com	没有服务器地理信息.
graph.qq.com	IP: 175.27.9.43 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
sdk.e.qq.com	IP: 119.147.13.93 所属国家: China 地区: Guangdong 城市: Shenzhen 纬度: 22.545540 经度: 114.068298
vop.baidu.com	IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
logs.amap.com	IP: 59.82.60.45 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423

URL信息	Url所在文件
https://api.weixin.qq.com/sns/oauth2/access_token?appid=	com/taobei/sandaier/wxapi/WXEntryActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/taobei/sandaier/wxapi/WXEntryActivity.java
http://city.ip138.com/ip2city.asp	com/lib/commonlib/utils/network/NetworkUtil.java
http://ip.taobao.com/service/getIpInfo.php?ip=myip	com/lib/commonlib/utils/network/NetworkUtil.java
http://127.0.0.1:3000	com/jtcf/http/httpClient.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/sdk/cons/C0098a.java
https://mobilegw.alipaydev.com/mgw.htm	com/alipay/sdk/cons/C0098a.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/cons/C0098a.java
https://wappaygw.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/C0098a.java
https://mclient.alipay.com/home/exterfaceAssign.htm?	com/alipay/sdk/cons/C0098a.java
https://mcgw.alipay.com/sdklog.do	com/alipay/sdk/packet/impl/C0119c.java
http://m.alipay.com/?action=h5quit	com/alipay/sdk/util/C0140l.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/data/C0101a.java
http://h5.m.taobao.com/trade/paySuccess.html?bizOrderId=\$OrderId\$&	com/alipay/sdk/data/RunnableC0102b.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/b/b/a.java
https://mobilegw.alipay.com/mgw.htm	com/alipay/b/b/a.java
http://mobilegw-1-64.test.alipay.net/mgw.htm	com/alipay/b/b/a.java

http://mobilegw.aaa.alipay.net/mgw.htm	com/alipay/b/b/a.java
https://paygate-yf.meituan.com/paygate/notify/alipay/paynotify/simple	com/alipay/test/a.java
http://mobilegw.stable.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://mobilegw.alipay.com/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.aaa.alipay.net/mgw.htm	com/alipay/apmobilesecuritysdk/b/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://lark.alipay.com/yj131525/byt0wl/ufnf3i#A10200	com/umeng/commonsdk/statistics/internal/c.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://developer.umeng.com/docs/66632/detail/70018?um_channel=sdk	com/umeng/analytics/b.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java

http://restapi.amap.com/v3/geocode/regeo	com/loc/bu.java
http://logs.amap.com/ws/log/upload? product=%s&type=%s&platform=%s&channel=%s&sign=%s	com/loc/u.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/db.java
http://apilocate.amap.com/mobile/binary	com/loc/cw.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cw.java
http://abroad.apilocate.amap.com/mobile/binary	com/loc/cp.java
http://apilocatesrc.amap.com/mobile/binary	com/loc/cp.java
https://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://restapi.amap.com/v3/iasdkauth	com/loc/l.java
http://cgicol.amap.com/collection/writedata?ver=v1.0_ali&	com/loc/cg.java
http://restapi.amap.com	com/loc/q.java
http://restapi.amap.com/v3/place/around?	com/loc/a.java
http://restapi.amap.com/v3/place/text?	com/loc/a.java
http://restapi.amap.com/v3/config/district?	com/loc/a.java
http://rqd.uu.qq.com/rqd/sync	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
http://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
www.qq.com	com/tencent/smtt/sdk/ag.java

http://pms.mb.qq.com/rsp204	com.tencent/smtt/sdk/ag.java
http://debugtbs.qq.com	com.tencent/smtt/sdk/WebView.java
http://debugx5.qq.com	com.tencent/smtt/sdk/WebView.java
http://debugtbs.qq.com?10000	com.tencent/smtt/sdk/WebView.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com.tencent/smtt/sdk/a/d.java
http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com.tencent/smtt/utls/v.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com.tencent/smtt/utls/v.java
http://wup.imtt.qq.com:8080	com.tencent/smtt/utls/v.java
http://log.tbs.qq.com/ajax?c=dl&k=	com.tencent/smtt/utls/v.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com.tencent/smtt/utls/v.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com.tencent/smtt/utls/v.java
http://mqqqad.html5.qq.com/adjs	com.tencent/smtt/utls/v.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com.tencent/smtt/utls/v.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com.tencent/smtt/utls/i.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%s	com.tencent/mm/opensdk/diffdev/a/f.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com.tencent/mm/opensdk/diffdev/a/d.java
https://graph.qq.com/oauth2.0/me	com.tencent/connect/UnionInfo.java

http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QQShare.java
http://fusion.qq.com/cgi-bin/qzapps/unified_jump?appid=%1\$s&from=%2\$s&isOpenAppID=1	com/tencent/connect/share/QzoneShare.java
https://openmobile.qq.com/oauth2.0/m_authorize?	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/user/user_login_statist	com/tencent/connect/auth/AuthAgent.java
https://openmobile.qq.com/v3/user/get_info	com/tencent/connect/auth/AuthAgent.java
http://appsupport.qq.com/cgi-bin/qzapps/mapp_addapp.cgi	com/tencent/connect/auth/AuthAgent.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/auth/a.java
http://openmobile.qq.com/oauth2.0/m_jump_by_version?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/login/qzsjump.html?	com/tencent/connect/common/BaseApi.java
http://qzs.qq.com/open/mobile/request/sdk_request.html?	com/tencent/open/SocialApilml.java
http://qzs.qq.com/open/mobile/invite/sdk_invite.html?	com/tencent/open/SocialApilml.java
http://qzs.qq.com/open/mobile/sendstory/sdk_sendstory_v1.3.html?	com/tencent/open/SocialApilml.java
http://qzs.qq.com	com/tencent/open/SocialApilml.java
https://huatuocode.huatuo.qq.com	com/tencent/open/b/d.java
https://openmobile.qq.com/	com/tencent/open/utis/HttpUtils.java
http://cgi.connect.qq.com/qqconnectopen/openapi/policy_conf	com/tencent/open/utis/f.java
http://wspeed.qq.com/w.cgi	com/qq/e/comm/services/RetCodeService.java
http://c.isdspeed.qq.com/code.cgi	com/qq/e/comm/services/RetCodeService.java

http://sdk.e.qq.com/err	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/activate	com/qq/e/comm/services/a.java
http://sdk.e.qq.com/launch	com/qq/e/comm/services/a.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/e.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/b/a/a.java
http://hydra.alibaba.com/	com/ta/utdid2/aid/AidRequester.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/XmlUtils.java
http://xmlpull.org/v1/doc/features.html#indent-output	com/ta/utdid2/core/persistent/FastXmlSerializer.java
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明	com/amap/api/location/AMapLocation.java
http://xiangliao.kaicd.com/share/shareWX	com/ixl/talk/xlmm/opensdk/constant/Constants.java
http://188.188.1.94:2018/api/gateway	com/ixl/talk/xlmm/opensdk/constant/Constants.java
https://data.iapppay.com/useractive	com/iapppay/utls/t.java
https://iapppay-data.iapppay.com/useractive	com/iapppay/utls/t.java
https://ipay.iapppay.com	com/iapppay/interfaces/network/HttpReqTask.java
https://payment.iapppay.com	com/iapppay/interfaces/network/HttpReqTask.java
https://iapppay.halodigit.com	com/iapppay/interfaces/network/HttpReqTask.java
http://127.0.0.1/	com/iapppay/interfaces/bean/OrderBean.java

http://data.iapppay.com:8048/domain?dn=data.iapppay.com	com/iapppay/service/logs/StatisticsUpload.java
https://data.iapppay.com/useractive	com/iapppay/service/logs/StatisticsUpload.java
https://iapppay-data.iapppay.com/useractive	com/iapppay/service/logs/StatisticsUpload.java
http://119.29.29.29/d?dn=	com/iapppay/apppaysystem/NetworkState.java
https://upfile.aiwaya.cn/uploadFile	com/cloudvoice/voice/lib/e/b.java
https://upfile.aiwaya.cn/speechDiscern	com/cloudvoice/voice/lib/e/b.java
http://117.50.17.160:8555/index	com/cloudvoice/voice/lib/e/b.java
http://wxqas.yayaim.com/tobot/test.html	com/cloudvoice/voice/lib/e/b.java
https://upfile.hqsuntek.com/uploadFile	com/cloudvoice/voice/lib/e/a.java
https://upfile.aiwaya.cn/speechDiscern	com/cloudvoice/voice/lib/e/a.java
https://voice.aiwaya.cn/index	com/cloudvoice/voice/lib/e/a.java
https://botserverh5.aiwaya.cn/index.html	com/cloudvoice/voice/lib/e/a.java
http://vop.baidu.com/open/asr	com/cloudvoice/voice/lib/common/baidu/Config.java
https://thirdwx.qlogo.cn	org/cocos2dx/lib/HeadTaskHandler.java
https://thirdwx.qlogo.cn	org/cocos2dx/lib/Cocos2dxDownloader.java
https://cdn.jtcfgames.com/protocol/yueyang/download/lcon-57.png	org/cocos2dx/javascript/Config.java
https://ssgw.updrips.com/oauth2/checkAppInfo	org/xianliao/im/sdk/net/model/LoginInfoRequest.java
http://120.24.210.161:52234/gateway/red/dispatcher	org/xianliao/im/sdk/net/model/GetBillIdlRequest.java

https://tsis.jpush.cn	cn/jiguang/c/a.java
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
http://example.com/	cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java
http://lame.sf.net	lib/armeabi/libbmp3lame.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi/libcocos2djs.so
https://www.openssl.org/docs/faq.html	lib/armeabi/libcocos2djs.so

邮箱线索

邮箱地址	所在文件
james@james-chen.local	lib/armeabi/libcocos2djs.so

手机线索

手机号	所在文件
13064875695	com/ixl/talk/xlmm/opensdk/openapi/XLApiImplComm.java

签名证书

APK is signed

v1 signature: True
v2 signature: False
v3 signature: False
Found 1 unique certificates
Subject: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-06-21 04:40:47+00:00
Valid To: 2077-03-24 04:40:47+00:00
Issuer: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown
Serial Number: 0x1f177132
Hash Algorithm: sha256
md5: 1cb3deb971f22181d970e91a0673e76a
sha1: bafe59b4412c098feb518e69803f5262b06e60c8
sha256: 7c99e2e264be2e023eff19e2fbf92d9d491e4a6ad3c9190962ee9f95101748da
sha512: f5f73d12026a90ce694a5ceb7d79ab7cea4f126c00f3f6a88483a325e834ba2b55765c6e320950f3263544cb3d091985f7e9416295263846046a697f38443387

硬编码敏感信息

可能的敏感信息
"ipay_password" : "密 码"
"ipay_ui_input_original_pwd" : "请输入原登录密码"
"ipay_ui_input_wrong_pwd" : "密码输入有误"
"ipay_ui_login_find_pwd" : "找回密码"
"ipay_ui_login_forget_pwd" : "忘记密码"
"ipay_ui_login_input_pwd" : "请输入密码"
"ipay_ui_login_input_pwd_again" : "请再次输入登录密码"

"ipay_ui_pwd_not_null" : "密码不能为空"
"ipay_ui_pwd_set" : "请输入6~24位登录密码"
"ipay_ui_reset_pwd" : "重置密码"
"ipay_ui_set_pwd" : "设置密码"
"ipay_ui_setting_pwd" : "正在设置密码..."

加壳分析

第三方SDK

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361
Bugly		https://reports.exodus-privacy.eu.org/trackers/190
JiGuang Aurora Mobile JPush	Analytics	https://reports.exodus-privacy.eu.org/trackers/343
Umeng Analytics		https://reports.exodus-privacy.eu.org/trackers/119

此APP的危险动作

	是否		
--	----	--	--

向手机申请的权限	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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.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
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.INTERACT_ACROSS_USERS_FULL	未知	Unknown permission	Unknown permission from android reference
android.permission.GET_TOP_ACTIVITY_INFO	未知	Unknown permission	Unknown permission from android reference
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
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.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.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.ACCESS_FINE_LOCATION	危险	精细定位（GPS）	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_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.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.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

应用内通信

活动(ACTIVITY)	通信(INTENT)
--------------	------------

org.cocos2dx.javascript.AppActivity	Schemes: @string/scheme://,
-------------------------------------	-----------------------------

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。