MoGua

None 6.0.5.APK 分析报告

APP名称:	None
包名:	vmiruem.cwnt.ajewmtkz
域名线索:	66条
URL线索:	72条

邮箱线索:	3条
分析日期:	2025年6月17日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: sg2hdf,das-ahjdg.apk
文件大小: 37.5MB
MD5值: 4c088d4b9fc3020ebe42a8b665bc2851
SHA1值: 5e16cd93ffab03ec4390e323505a99fdd6137261
SHA256值: c1b84e19566348efbbd91f8ed1fd35a349866dcc55ac4fa301873611cad247d4

APP 信息

App名称: None
包名: vmiruem.cwnt.ajewmtkz
主活动Activity: com.izofficeu.syyizoff.ivbjwejwhcvaktvtcActivity
安卓版本名称: 6.0.5
安卓版本: 1

域名线索

域名	服务器信息
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
opentest.bmob.cn	没有服务器地理信息.
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
lbs.netease.im	**IP**: 220.197.34.89 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
h.trace.qq.com	**IP**: 113.56.189.162 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
www.bjtime.cn	没有服务器地理信息.
www.jivesoftware.com	**IP**: 23.235.209.143 **所属国家**: United States of America **地区**: Virginia **城市**: Virginia Beach **纬度**: 36.837925 **经度**: -76.093918
norma-external-collect.meizu.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
open3.bmob.cn	没有服务器地理信息

open3.bmob.cn	没有服务器地理信息.
p0.api.upyun.com	**IP**: 101.251.144.15 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
open.weixin.qq.com	**IP**: 140.207.121.14 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
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
cfg.imtt.qq.com	**IP**: 60.28.172.238 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
qyqa.netease.com	**IP**: 59.111.96.241 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
59.111.110.241	**IP**: 59.111.110.241 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
xmlpull.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 116.78.120.73

www.jd.com	**所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
goo.gl	IP: 173.194.202.113 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
wup.imtt.qq.com	IP: 125.39.104.63 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
m.toutiao.com	IP: 125.39.135.107 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
file.bmob.cn	没有服务器地理信息.
www.bouncycastle.org	IP: 43.250.142.130 **所属国家**: Australia **地区**: Queensland **城市**: Warren **纬度**: -23.500000 **经度**: 150.283325
app.bmob.iwyttc.com	IP: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
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

v0.api.upyun.com	**IP**: 218.28.104.157 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
m0.api.upyun.com	**IP**: 218.28.104.157 **所属国家**: China **地区**: Henan **城市**: Zhengzhou **纬度**: 34.757778 **经度**: 113.648613
imtest.netease.im	**IP**: 111.124.202.79 **所属国家**: China **地区**: Guizhou **城市**: Zunyi **纬度**: 27.686441 **经度**: 106.907135
statistic.live.126.net	**IP**: 220.197.34.76 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
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
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
android.bugly.qq.com	**IP**: 124.95.225.146 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
	IP: 210.72.145.8 **所属国家**: China

www.time.ac.cn	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.qq.com	**IP**: 221.198.70.47 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
resolver.msg.global.xiaomi.net	**IP**: 34.36.192.126 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
imtest6.netease.im	没有服务器地理信息.
www.baidu.com	**IP**: 110.242.69.21 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
schemas.android.com	没有服务器地理信息.
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
www.ntsc.ac.cn	**IP**: 159.226.242.43 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

io.codenow.cn	**IP**: 106.75.70.127 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
ip-api.com	**IP**: 208.95.112.1 **所属国家**: United States of America **地区**: North Carolina **城市**: Skyland **纬度**: 35.483757 **经度**: -82.521996
dr.netease.im	**IP**: 220.197.34.84 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
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
nrtc.netease.im	**IP**: 220.197.34.72 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
register.xmpush.global.xiaomi.com	**IP**: 47.237.96.1 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
mqqad.html5.qq.com	**IP**: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 101.72.202.200 **所属国家**: China

www.taobao.com	**所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
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
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
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
roomserver.netease.im	IP: 220.197.34.72 **所属国家**: China **地区**: Sichuan **城市**: Leshan **纬度**: 29.562281 **经度**: 103.763863
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
ru.register.xmpush.global.xiaomi.com	IP: 107.155.52.56 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752258 **经度**: 37.615471
soft.tbs.imtt.qq.com	IP: 119.167.147.86 **所属国家**: China **地区**: Shandong **城市**: Qingdao

	纬度: 36.098610 **经度**: 120.371941
astat.bugly.qcloud.com	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
maps.google.cn	IP: 114.250.65.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
wannos.127.net	IP: 45.127.129.16 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
fr.register.xmpush.global.xiaomi.com	IP: 98.64.182.160 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
nosup-hz1.127.net	IP: 175.19.125.207 **所属国家**: China **地区**: Jilin **城市**: Changchun **纬度**: 43.880001 **经度**: 125.322777
p.bmob.cn	没有服务器地理信息.
idmb.register.xmpush.global.xiaomi.com	IP: 20.219.205.9 **所属国家**: India **地区**: Maharashtra **城市**: Pune **纬度**: 18.519663

	经度: 73.854507
imtest4.netease.im	**IP**: 59.111.241.163 **所属国家**: China **地区**: Guangdong **城市**: Guangzhou **纬度**: 23.127361 **经度**: 113.264572
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

URL线索

URL**信息**	Url**所在文件**
https://h.trace.qq.com/kv	EEvjbonVNZ1tF7KIKSgn/FhLYLIolwDgmFEE8uXEv/KBToqlIvx6i9Lo6zvRvj/EEvjbonVNZ1tF7KIKSgn/C0446.java
https://astat.bugly.qcloud.com/rqd/async	EEvjbonVNZ1tF7KIKSgn/FhLYLIolwDgmFEE8uXEv/KBToqlIvx6i9Lo6zvRvj/EEvjbonVNZ1tF7KIKSgn/C0428.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	EEvjbonVNZ1tF7KIKSgn/FhLYLIolwDgmFEE8uXEv/KBToqlIvx6i9Lo6zvRvj/EEvjbonVNZ1tF7KIKSgn/C0428.java
http://m.toutiao.com	EEvjbonVNZ1tF7KIKSgn/b7F1IRgibohql2p6uK6e/KBToqlIvx6i9Lo6zvRvj/C1021.java
http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red	EEvjbonVNZ1tF7KIKSgn/b7F1IRgibohql2p6uK6e/KBToqlIvx6i9Lo6zvRvj/FIdvQ6JPnKFHN4HtFJVr/KBToqlIvx6i9Lo6zvRvj/InterfaceC0778.java
https://play.google.com/store/apps/details?id=	EEvjbonVNZ1tF7KIKSgn/FIdvQ6JPnKFHN4HtFJVr/KBToqlIvx6i9Lo6zvRvj/b7F1IRgibohql2p6uK6e/C0169.java
http://xml.apache.org/xslt	EEvjbonVNZ1tF7KIKSgn/J3zZDZADwBwe7PYo2VRz/KBToqlIvx6i9Lo6zvRvj/C0518.java
http://127.0.0.1	EEvjbonVNZ1tF7KIKSgn/Vp4nqOaAaO5yOLsMS2EK/KBToqlIvx6i9Lo6zvRvj/KBToqlIvx6i9Lo6zvRvj/EEvjbonVNZ1tF7KIKSgn/AbstractC0635.java
http://www.bjtime.cn	EEvjbonVNZ1tF7KIKSgn/vcnYLpC8eYCZ8cKGmYST/KBToqlIvx6i9Lo6zvRvj/QkUfIbVoQR8KNYDXBbIx/C2237.java
http://www.baidu.com	EEvjbonVNZ1tF7KIKSgn/vcnYLpC8eYCZ8cKGmYST/KBToqlIvx6i9Lo6zvRvj/QkUfIbVoQR8KNYDXBbIx/C2237.java
http://www.taobao.com	EEvjbonVNZ1tF7KIKSgn/vcnYLpC8eYCZ8cKGmYST/KBToqlIvx6i9Lo6zvRvj/QkUfIbVoQR8KNYDXBbIx/C2237.java

http://www.ntsc.ac.cn	EEvjbonVNZ1tF7KIKSgn/vcnYLpC8eYCZ8cKGmYST/KBToqIlvx6i9Lo6zvRvj/QkUflbVoQR8KNYDXBbIx/C2237.java
http://www.time.ac.cn/	EEvjbonVNZ1tF7KIKSgn/vcnYLpC8eYCZ8cKGmYST/KBToqIlvx6i9Lo6zvRvj/QkUflbVoQR8KNYDXBbIx/C2237.java
http://xml.apache.org/xslt	EEvjbonVNZ1tF7KIKSgn/xxeoGzPoSYg16gQl7wve/KBToqIlvx6i9Lo6zvRvj/C2317.java
http://www.bouncycastle.org)	OSRuAhZvRfgQY45e5LK2/vLAkcQnctHsIhRToKYFs/C3962.java
http://...	OSRuAhZvRfgQY45e5LK2/dbZfwlHOWmGbgMQXKQkW/KBToqIlvx6i9Lo6zvRvj/KBToqIlvx6i9Lo6zvRvj/C2609.java
http://m0.api.upyun.com	cn/bmob/v3/datatype/up/UpConfig.java
http://v0.api.upyun.com	cn/bmob/v3/datatype/up/UpConfig.java
http://v0.api.upyun.com/	cn/bmob/v3/datatype/up/FormUploader.java
http://m0.api.upyun.com/	cn/bmob/v3/datatype/up/BlockUploader.java
https://v0.api.upyun.com	cn/bmob/v3/datatype/up/ParallelUploader.java
http://p0.api.upyun.com/pretreatment/	cn/bmob/v3/datatype/up/ParallelUploader.java
http://p.bmob.cn/8/	cn/bmob/v3/http/BmobURL.java
https://opentest.bmob.cn/8/	cn/bmob/v3/http/BmobURL.java
https://open3.bmob.cn/8/	cn/bmob/v3/http/BmobURL.java
http://file.bmob.cn	cn/bmob/v3/http/BmobURL.java
http://io.codenow.cn:3010	cn/bmob/v3/http/BmobURL.java
http://io.codenow.cn:3010/socket.io/1/	cn/bmob/v3/realtime/Client.java
http://io.codenow.cn:3010/socket.io/1/websocket/	cn/bmob/v3/realtime/Client.java
http://io.codenow.cn	cn/bmob/v3/realtime/Client.java
http://app.bmob.iwyttc.com/8/	com/ddtx/dingdatacontact/Entity/AppData.java
http://qyqa.netease.com	com/ddtx/dingdatacontact/main/activity/PrivatizationConfigActivity.java
http://59.111.110.241:10081/lbs/demoConfig.jsp	com/ddtx/dingdatacontact/main/activity/PrivatizationConfigActivity.java
https://api.weixin.qq.com/sns/userinfo?access_token=	com/ddtx/dingdatacontact/login/LoginActivity.java

http://ip-api.com/json/?lang=zh-CN	com/ddtx/dingdatacontact/login/LoginActivity.java
https://api-push.meizu.com	com/meizu/cloud/pushsdk/b/c/e.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
http://norma-external-collect.meizu.com/android/exchange/getpublickey.do	com/meizu/cloud/pushsdk/a/a/a.java
http://norma-external-collect.meizu.com/push/android/external/add.do	com/meizu/cloud/pushsdk/a/a/b.java
https://www.baidu.com/index.php?tn=25017023_10_pg&ssl_s=1&ssl_c=ssl1_171a56a2313&prec=1	com/netease/nim/uikit/business/session/activity/fragment/BaiFragment.java
https://www.jd.com/	com/netease/nim/uikit/business/session/activity/fragment/JingFragment.java
https://www.qq.com/	com/netease/nim/uikit/business/session/activity/fragment/TengFragment.java
https://api.weixin.qq.com/sns/oauth2/access_token	com/netease/nim/uikit/rest/Host.java
http://statistic.live.126.net/statics/report/common/form	com/netease/nimlib/c/f/a.java
http://statistic.live.126.net/statics/report/im/sdk/msgreceived	com/netease/nimlib/session/h.java
https://imtest.netease.im/lbs/conf.jsp	com/netease/nimlib/e/e.java
https://imtest.netease.im/1.gif	com/netease/nimlib/e/e.java
https://imtest4.netease.im/test	com/netease/nimlib/e/e.java
https://imtest6.netease.im:8012/	com/netease/nimlib/e/e.java
https://imtest.netease.im/lbsrc/conf.jsp	com/netease/nimlib/e/e.java
https://lbs.netease.im/lbs/conf.jsp	com/netease/nimlib/e/e.java
https://dr.netease.im/1.gif	com/netease/nimlib/e/e.java
http://wannos.127.net/lbs;http://wannos-hz.127.net/lbs;http://wannos-bj.127.net/lbs;http://wannos-oversea.127.net/lbs;http://223.252.196.38/lbs	com/netease/nimlib/e/g.java
https://nrtc.netease.im/nrtc/detect.action	com/netease/nrtc/NetDetector.java
https://nrtc.netease.im/nrtc/rejoin.action	com/netease/nrtc/a.java

https://nrtc.netease.im/nrtc/getChannelInfos.action	com/netease/nrtc/b.java
https://roomserver.netease.im/v1/sdk/command/rooms	com/netease/nrtc/engine/impl/h.java
https://statistic.live.126.net/statistic/realtime/sdkinfo	com/netease/nrtc/engine/impl/e.java
https://lbs.netease.im/cc/nrtc/v2	com/netease/nrtc/engine/impl/e.java
https://lbs.netease.im/cc/nrtc/v2	com/netease/nrtc/engine/rawapi/IRtcEngine.java
https://statistic.live.126.net/statistic/realtime/sdkFunctioninfo	com/netease/nrtc/monitor/d.java
https://statistic.live.126.net/statistic/realtime/sdkinfo	com/netease/nrtc/monitor/j.java
https://goo.gl/FE5SeB	com/netease/nrtc/utility/l.java
https://nrtc.netease.im/nrtc/uploadSdkLog.action	com/netease/nrtc/utility/b/a.java
https://wannos.127.net/lbs	com/netease/yunxin/nos/sdk/NosComponent.java
https://statistic.live.126.net/sdklog/getToken	com/netease/yunxin/nos/sdk/NosComponent.java
https://nosup-hz1.127.net	com/netease/yunxin/nos/sdk/NosComponent.java
https://statistic.live.126.net/statics/report/common/form	com/netease/yunxin/report/sdk/ReportComponent.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.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://pms.mb.qq.com/rsp204	com/tencent/smtt/sdk/j.java
http://mdc.html5.qq.com/mh?channel_id=50079&u=	com/tencent/smtt/sdk/a/c.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11047	com/tencent/smtt/sdk/b/a/a.java
http://mdc.html5.qq.com/d/directdown.jsp?channel_id=11041	com/tencent/smtt/sdk/b/a/a.java

http://log.tbs.qq.com/ajax?c=pu&v=2&k=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utils/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utils/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utils/n.java
http://mqqad.html5.qq.com/adjs	com/tencent/smtt/utils/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utils/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utils/d.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fr.java
http://www.jivesoftware.com/xmlns/xmpp/properties\	com/xiaomi/push/gc.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/gj.java
https://%1$s/gslb/?ver=4.0	com/xiaomi/push/cs.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/gk.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/ff.java
https://resolver.msg.global.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bj.java
https://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/bj.java
https://cn.register.xmpush.xiaomi.com	com/xiaomi/push/service/m.java
https://register.xmpush.global.xiaomi.com	com/xiaomi/push/service/m.java

https://fr.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/m.java
https://ru.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/m.java
https://idmb.register.xmpush.global.xiaomi.com	com/xiaomi/push/service/m.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/AbstractC7531.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/AbstractC7503.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/AbstractC7544.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/AbstractC7536.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/AbstractC7502.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/ht2O656ZGts3zSKlR9hi/C6001.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	dbZfwlHOWmGbgMQXKQkW/KBToqlIvx6i9Lo6zvRvj/ht2O656ZGts3zSKlR9hi/C5992.java
http://schemas.android.com/apk/res/android	vcnYLpC8eYCZ8cKGmYST/Cnbr2w6ysdD5bn3Uw96P/EEvjbonVNZ1tF7KIKSgn/y7MjNXD1VMUfDeGnnL1Q/C7747.java

邮箱线索

邮箱地址	所在文件
hyy@189.cn hyy@gmail.com 732662@sina.com hyy12@qq.com hyy-123@163.com hyy@hotmail.com hyy@139.com hyy@sohu.com	EEvjbonVNZ1tF7KIKSgn/FIdvQ6JPnKFHN4HtFJVr/KBToqlIvx6i9Lo6zvRvj/J3zZDZADwBwe7PYo2VRz/C0130.java
rubin@rubindemacbook-pro.local	com/netease/yunxin/nos/sdk/NosFacade.java
rubin@rubindemacbook-pro.local	com/netease/yunxin/report/sdk/ReportManager.java

手机线索

手机号	所在文件
17179869184	OSRuAhZvRfgQY45e5LK2/vLAkcQnctHsIhRToKYFs/b7F1IRgibohql2p6uK6e/vLAkcQnctHsIhRToKYFs/KBToqIlvx6i9Lo6zvRvj/C2715.java
17179869183	OSRuAhZvRfgQY45e5LK2/vLAkcQnctHsIhRToKYFs/b7F1IRgibohql2p6uK6e/vLAkcQnctHsIhRToKYFs/KBToqIlvx6i9Lo6zvRvj/C2715.java
15095675534	OSRuAhZvRfgQY45e5LK2/vLAkcQnctHsIhRToKYFs/vcnYLpC8eYCZ8cKGmYST/olaRj5F69gcVy52CKnsL/C3846.java
13000000000	com/ddtx/dingdatacontact/main/activity/FeedBackActivity.java
13000000000	com/netease/nim/uikit/complaint/ReportActivity.java

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=yaZxG, ST=Whon6, L=d9II7, O=sf1749983817618, OU=xd1749983817618, CN=beko
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-15 10:36:58+00:00
有效期至: 2075-06-03 10:36:58+00:00
发行人: C=yaZxG, ST=Whon6, L=d9II7, O=sf1749983817618, OU=xd1749983817618, CN=beko
序列号: 0x2c4517a5
哈希算法: sha512
md5值: 4a126d4d50c4703f4c2851e187b3362e
sha1值: 0c73a37cbe00bbd00b5cdd30b2ad9d8a18dd6826
sha256值: 49ed9a247b0cb5fc755fc4631226bfe02ee66e2d38c68f1689f3848556788626
sha512值: 9f4dcfeea5e4bc710696e8c1c46098ca46de6a20006dc68cc5c6629b44877ee36400047fdf9c264d740561db9dee6be2b617430eadc09663fc2242df3163a463
公钥算法: rsa
密钥长度: 4096
指纹: 8da480242b790ffe69bfc0ea44e848ed74b527220e4d61b1eb437fe7e0db17c2

硬编码敏感信息

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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_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.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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器

android.permission.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
vmiruem.cwnt.ajewmtkz.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.heytap.mcs.permission.RECIEVE_MCS_MESSAGE	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
vmiruem.cwnt.ajewmtkz_com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.meizu.c2dm.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
android.permission.PROCESS_OUTGOING_CALLS	危险	拦截拨出电话	允许应用程序处理拨出电话并更改要拨打的号码。恶意应用程序可能会监控,重定向或阻止拨出电话
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.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.ANSWER_PHONE_CALLS	危险		允许应用接听来电。
android.permission.READ_CALL_LOG	危险		允许应用程序读取用户的通话日志
android.permission.WRITE_CALL_LOG	危险		允许应用程序写入（但不读取）用户号召日志数据。
android.permission.KILL_BACKGROUND_PROCESSES	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
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
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
vmiruem.cwnt.ajewmtkz_com.sec.android.provider.badge.permission.READ	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.sec.android.provider.badge.permission.WRITE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.htc.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.htc.launcher.permission.UPDATE_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.sonyericsson.home.permission.BROADCAST_BADGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.anddoes.launcher.permission.UPDATE_COUNT	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.majeur.launcher.permission.UPDATE_BADGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.huawei.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
		Unknown	

vmiruem.cwnt.ajewmtkz_com.huawei.android.launcher.permission.WRITE_SETTINGS	未知	permission	Unknown permission from android reference
android.permission.READ_APP_BADGE	正常	显示应用程序通知	允许应用程序显示应用程序图标徽章
vmiruem.cwnt.ajewmtkz_com.oppo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_com.oppo.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz_me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
vmiruem.cwnt.ajewmtkz.permission.PUSH_PROVIDER	未知	Unknown permission	Unknown permission from android reference
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。
vmiruem.cwnt.ajewmtkz_com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

应用内通信