



MoGua

博文 1.1.3.APK 分析报告



APP名称:	博文
包名:	com.vexqqn.azczhwhx
域名线索:	77条
URL线索:	78条
邮箱线索:	3条

分析日期:2025年7月17日

分析平台:[摸瓜APK反编译平台](#)

文件信息

文件名: 5_base.apk
文件大小: 40.08MB
MD5值: 6b8acf383b76c3c255836921ac7a68fa
SHA1值: c47d53f32c4916474dbff5df9c920be09d82f412
SHA256值: 2691ea874526a0294f9387ffe55db171c3be1b12c0baf42e1d5f22c737586a21

APP 信息

App名称: 博文
包名: com.vexqqn.azczhwhx
主活动Activity: com.VnwcWKHib.kxLWDkDWLnalEI.hyxovpdzupfwyActivity
安卓版本名称: 1.1.3
安卓版本: 1

域名线索

域名	服务器信息

imtest6.netease.im	没有服务器地理信息.
lbs.netease.im	IP: 45.254.49.32 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
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
nosup-hz1.127.net	IP: 45.127.129.8 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
schemas.android.com	没有服务器地理信息.
play.google.com	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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

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
store.hispace.hicloud.com	IP: 123.249.62.130 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
app.bmob.iwyttc.com	没有服务器地理信息.
nrtc.netease.im	IP: 47.96.190.103 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
pms.mb.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
opentest.bmob.cn	没有服务器地理信息.
register.xmpush.global.xiaomi.com	IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
grs.dbankcloud.cn	IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
m0.api.upyun.com	IP: 218.60.175.252 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722

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
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
file.bmob.cn	没有服务器地理信息.
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
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
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
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
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
	IP: 60.29.240.122 所属国家: China

mdc.html5.qq.com	地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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
dr.netease.im	IP: 101.71.139.136 所属国家: China 地区: Zhejiang 城市: Ningbo 纬度: 29.878410 经度: 121.549767
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
roomserver.netease.im	IP: 47.96.190.103 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
goo.gl	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
imtest.netease.im	IP: 59.111.209.232 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.bjtime.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

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
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
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
grs.dbankcloud.asia	IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
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
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
	IP: 0.0.0.1 所属国家: - 地区: -

mqqad.html5.qq.com	城市:- 纬度: 0.000000 经度: 0.000000
open.weixin.qq.com	IP: 223.167.82.219 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
m.toutiao.com	IP: 182.40.61.216 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
www.jd.com	IP: 123.6.77.65 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
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
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
resolver.msg.global.xiaomi.net	IP: 8.219.74.181 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.openssl.org	IP: 34.36.58.177 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568

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
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
grs.dbankcloud.eu	没有服务器地理信息.
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
p.bmob.cn	没有服务器地理信息.
wannos.127.net	IP: 223.252.196.42 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.taobao.com	IP: 61.182.130.193 所属国家: China 地区: Hebei 城市: Zhangjiakou 纬度: 40.810024 经度: 114.879349
www.baidu.com	IP: 110.242.68.3 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
grs.dbankcloud.com	IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji 纬度: 34.353611 经度: 107.375275

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
www.bouncycastle.org	IP: 203.32.61.103 所属国家: Australia 地区: Victoria 城市: Drouin 纬度: -38.136581 经度: 145.858383
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
resolver.msg.xiaomi.net	IP: 111.202.1.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
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
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
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
v0.api.upyun.com	IP: 218.60.175.252 所属国家: China 地区: Liaoning 城市: Dandong 纬度: 40.129169 经度: 124.394722
norma-external-collect.meizu.com	IP: 183.60.176.112 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
open3.bmob.cn	没有服务器地理信息.
statistic.live.126.net	IP: 101.71.139.161 所属国家: China 地区: Zhejiang 城市: Ningbo 纬度: 29.878410 经度: 121.549767
cn.register.xmpush.xiaomi.com	IP: 111.202.1.240 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
appgallery.cloud.huawei.com	IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou

	纬度: 23.127361 经度: 113.264572
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
www.time.ac.cn	IP: 210.72.145.8 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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

 URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	YTSQe1ys7zUTWm1W5F4b/tF2eNITcjQ8TXD7qsjsG/ckNlwYDypKyM5FPmGZ4t/gjCIE3gxDZbFjPTriaBh/C1338.java
http://127.0.0.1	ckNlwYDypKyM5FPmGZ4t/PYxA7RJTP4lfhefMfaNc/gl38SVNG2KZpFvuqFleF/gl38SVNG2KZpFvuqFleF/ckNlwYDypKyM5FPmGZ4t/AbstractC2821.java
http://xml.apache.org/xslt	ckNlwYDypKyM5FPmGZ4t/YwcgpkQgURXBp9MKACf/gl38SVNG2KZpFvuqFleF/C2865.java
http://www.bjtime.cn	ckNlwYDypKyM5FPmGZ4t/aOPC4z5PzTtckRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzIKH2fgvN9gMzn/C2886.java
http://www.baidu.com	ckNlwYDypKyM5FPmGZ4t/aOPC4z5PzTtckRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzIKH2fgvN9gMzn/C2886.java
http://www.taobao.com	ckNlwYDypKyM5FPmGZ4t/aOPC4z5PzTtckRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzIKH2fgvN9gMzn/C2886.java
http://www.ntsc.ac.cn	ckNlwYDypKyM5FPmGZ4t/aOPC4z5PzTtckRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzIKH2fgvN9gMzn/C2886.java
http://www.time.ac.cn/	ckNlwYDypKyM5FPmGZ4t/aOPC4z5PzTtckRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzIKH2fgvN9gMzn/C2886.java
http://xml.apache.org/xslt	ckNlwYDypKyM5FPmGZ4t/nFdl4qFibYdUYjry1rCD/gl38SVNG2KZpFvuqFleF/C3739.java
https://play.google.com/store/apps/details?id=	ckNlwYDypKyM5FPmGZ4t/oElouTRrYHY9pXT3mUdM/gl38SVNG2KZpFvuqFleF/YwcgpkQgURXBp9MKACf/C3932.java

https://astat.bugly.qcloud.com/rqd/async	ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21flwIMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4157.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21flwIMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4157.java
https://h.trace.qq.com/kv	ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21flwIMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4103.java
http://m.toutiao.com	ckNIwYDypKyM5FPmGZ4t/wDHeulSM4rsILeyqcmiC/gl38SVNG2KZpFvuqFleF/C4690.java
http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red	ckNIwYDypKyM5FPmGZ4t/wDHeulSM4rsILeyqcmiC/gl38SVNG2KZpFvuqFleF/oEloUTRrYHY9pXT3mUdM/gl38SVNG2KZpFvuqFleF/AbstractC4560.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
http://m0.api.upyun.com	cn/bmob/v3/datatype/up/UpConfig.java
http://v0.api.upyun.com	cn/bmob/v3/datatype/up/UpConfig.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
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
http://59.111.110.241:10081/lbs/demoConfig.jsp	com/ddtx/dingdatacontact/main/activity/PrivatizationConfigActivity.java

http://qyqa.netease.com	com/ddtx/dingdatacontact/main/activity/PrivatizationConfigActivity.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SlidingTabLayout.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/CommonTabLayout.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://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
https://www.baidu.com/index.php?tn=25017023_10_pg&ssl_s=1&ssl_c=ssl_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
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
http://statistic.live.126.net/statics/report/im/sdk/msgreceived	com/netease/nimlib/session/h.java

https://nrtc.netease.im/nrtc/rejoin.action	com/netease/nrtc/a.java
https://nrtc.netease.im/nrtc/detect.action	com/netease/nrtc/NetDetector.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
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×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.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/utills/n.java
http://log.tbs.qq.com/ajax?c=pu&tk=	com/tencent/smtt/utills/n.java
http://wup.imtt.qq.com:8080	com/tencent/smtt/utills/n.java
http://log.tbs.qq.com/ajax?c=dl&k=	com/tencent/smtt/utills/n.java
http://cfg.imtt.qq.com/tbs?v=2&mk=	com/tencent/smtt/utills/n.java
http://log.tbs.qq.com/ajax?c=ul&v=2&k=	com/tencent/smtt/utills/n.java
http://mqqqad.html5.qq.com/ads	com/tencent/smtt/utills/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utills/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utills/d.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/fr.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/ff.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
http://xmlpull.org/v1/doc/features.html	com/xiaomi/push/gk.java
https://%1\$s/gslb/?ver=4.0	com/xiaomi/push/cs.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
http://www.bouncycastle.org)	rb9RtYti3qujsUEAlFON/aOPC4z5PzTttcKRXizg9/C7549.java
http://...	rb9RtYti3qujsUEAlFON/wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/gl38SVNG2KZpFvuqFleF/C7641.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9318.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9336.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9350.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9338.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9342.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/KJCeBaZNoHMe52vPYFMW/C7731.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	wDHeuISM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/KJCeBaZNoHMe52vPYFMW/C7733.java
https://play.google.com/store	Mogua Engine V1
https://appgallery.cloud.huawei.com/app/	Mogua Engine V1
https://play.google.com/store/apps/details?id=	Mogua Engine V1
https://appgallery.cloud.huawei.com	Mogua Engine V1
https://store.hispace.hicloud.com/hwmarket/api/	Mogua Engine V1
https://metrics1.data.hicloud.com:6447	Mogua Engine V2
https://metrics-dra.dt.hicloud.com:6447	Mogua Engine V2
https://metrics2.data.hicloud.com:6447	Mogua Engine V2
https://metrics5.data.hicloud.com:6447	Mogua Engine V2
https://grs.dbankcloud.com	Mogua Engine V2
https://grs.dbankcloud.cn	Mogua Engine V2
https://grs.dbankcloud.eu	Mogua Engine V2
https://grs.dbankcloud.asia	Mogua Engine V2

https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/libsmcderxrpcbv.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/librts_network.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libnrtc_sdk.so

✉ 邮箱线索

邮箱地址	所在文件
hyy@gmail.com hyy-123@163.com hyy@189.cn hyy@sohu.com 732662@sina.com hyy12@qq.com hyy@139.com hyy@hotmail.com	ckNIwYDypKyM5FPmGZ4t/oEIoUTRrYHY9pXT3mUdM/gl38SVNG2KZpFvuqFleF/HNC5dUqKvaNpTs8yeopp/C3896.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
13000000000	com/ddtx/dingdatacontact/main/activity/FeedBackActivity.java
17535567345	com/netease/nim/uikit/business/session/module/input/InputPanel.java
13000000000	com/netease/nim/uikit/complaint/ReportActivity.java
15095675534	rb9RtYti3qujsUEAIFON/aOPC4z5PzTttcKRXizg9/YTSQe1ys7zUTWm1W5F4b/NA1EwEaukKKIRZSgebMM/C6365.java
17179869184	rb9RtYti3qujsUEAIFON/aOPC4z5PzTttcKRXizg9/YwcgpkQgURXBp9MKACf/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/C6931.java
17179869183	rb9RtYti3qujsUEAIFON/aOPC4z5PzTttcKRXizg9/YwcgpkQgURXBp9MKACf/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/C6931.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=MiiPcCub, ST=NoYKOWwn, L=RrQEBQSP, O=MFdZfNnh, OU=OXKGgUGu, CN=zuxlQoIF
签名算法: rsassa_pkcs1v15
有效期自: 2024-03-17 02:35:42+00:00
有效期至: 2034-03-15 02:35:42+00:00
发行人: C=MiiPcCub, ST=NoYKOWwn, L=RrQEBQSP, O=MFdZfNnh, OU=OXKGgUGu, CN=zuxlQoIF
序列号: 0xc7ac05b8b5f42ea8
哈希算法: sha256
md5值: 9cbac757b992af42f8adb8dc2ec73366
sha1值: 38b35aa6eb5005829efbbc4acd825391f0c214fc
sha256值: 1e5d5b65b64bacecb149146b196d83b71fd0f212f03fefbbd0a97e92ea3000d7
sha512值: 791794986b6336ab8150b7c7a68fd29cf90011d272558cea48c3506500f12037862f9a86750220e238355a0dc07ba4e72cb3bd18467e4c594e03e5fa6d824896
公钥算法: rsa
密钥长度: 2048
指纹: 82f10a4f76616e3601e96682227818f13ba720afc17bff4e1ccfdee9d6a597f7

硬编码敏感信息

可能的敏感信息
"input_password" : "请输入密码，6~20位字母或者数字"
"main_tab_session" : "会话"
"nrtc_setting_other_device_default_rotation_key" : "nrtc_setting_other_device_default_rotation_key"
"nrtc_setting_other_device_rotation_fixed_offset_key" : "nrtc_setting_other_device_rotation_fixed_offset_key"
"nrtc_setting_other_server_record_audio_key" : "nrtc_setting_other_server_record_audio_key"
"nrtc_setting_other_server_record_video_key" : "nrtc_setting_other_server_record_video_key"
"nrtc_setting_vie_crop_ratio_key" : "nrtc_setting_vie_crop_ratio_key"
"nrtc_setting_vie_default_front_camera_key" : "nrtc_setting_vie_default_front_camera_key"
"nrtc_setting_vie_fps_reported_key" : "nrtc_setting_vie_fps_reported_key"
"nrtc_setting_vie_hw_decoder_key" : "nrtc_setting_vie_hw_decoder_key"
"nrtc_setting_vie_hw_encoder_key" : "nrtc_setting_vie_hw_encoder_key"
"nrtc_setting_vie_max_bitrate_key" : "nrtc_setting_vie_max_bitrate_key"

"nrtc_setting_vie_quality_key" : "nrtc_setting_vie_quality_key"
"nrtc_setting_vie_rotation_key" : "nrtc_setting_vie_rotation_key"
"nrtc_setting_voe_audio_aec_key" : "nrtc_setting_voe_audio_aec_key"
"nrtc_setting_voe_audio_ns_key" : "nrtc_setting_voe_audio_ns_key"
"nrtc_setting_voe_call_proximity_key" : "nrtc_setting_voe_call_proximity_key"
"nrtc_setting_voe_high_quality_key" : "nrtc_setting_voe_high_quality_key"
"please_input_confirm_pwd" : "请确认密码"
"please_input_pwd" : "请设置密码"
"private_config_note" : " 1.私有化配置的将在app重启后生效，请注销登陆并杀掉进程。 2.如果要切换到环境， 关闭或打开开关退出登陆杀掉进程即可。 "
"setting_private_config" : "私有化配置"
"team_authentication" : "身份验证"
"team_invitee_authentication" : "被邀请人身份验证"
"team_invitee_need_authen" : "需要验证"
"team_invitee_not_need_authen" : "不需要验证"
"team_need_authentication" : "需要身份验证"
"tui_user" : "推荐人员"

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

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。
com.VnwcWKHib.kxLWDkDWLnalEI.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
com.VnwcWKHib.kxLWDkDWLnalEI.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.VnwcWKHib.kxLWDkDWLnalEI.permission.C2D_MESSAGE	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
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
com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
com.VnwcWKHib.kxLWDkDWLnalEI.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
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

com.sec.android.provider.badge.permission.READ	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.sec.android.provider.badge.permission.WRITE	正常	在应用程序上显示通知计数	在三星手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.htc.launcher.permission.UPDATE_SHORTCUT	正常	在应用程序上显示通知计数	在 htc 手机的应用程序启动图标上显示通知计数或徽章。
com.sonyericsson.home.permission.BROADCAST_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	正常	在应用程序上显示通知计数	在索尼手机的应用程序启动图标上显示通知计数或徽章。
com.anddoes.launcher.permission.UPDATE_COUNT	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或徽章
com.majeur.launcher.permission.UPDATE_BADGE	正常	在应用程序上显示通知计数	在应用程序启动图标上显示通知计数或标记为固体。
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.huawei.android.launcher.permission.READ_SETTINGS	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.huawei.android.launcher.permission.WRITE_SETTINGS	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
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
com.oppo.launcher.permission.READ_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
com.oppo.launcher.permission.WRITE_SETTINGS	正常	在应用程序上显示通知计数	在oppo手机的应用程序启动图标上显示通知计数或徽章。
me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
com.VnwcWKHib.kxLWDkDWLnalEI.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference

com.VnwcWKHib.kxLWDkDWLnalEl.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。
com.huawei.appmarket.service.commondata.permission.GET_COMMON_DATA	未知	Unknown permission	Unknown permission from android reference

应用内通信

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。