



MoGua

TG 2.88.7.APK 分析报告



APP名称:	TG
包名:	tCgzvUhmcW.axmsdn.swjpfjs.slzpslgt
域名线索:	78条
URL线索:	79条
邮箱线索:	3条

分析日期:

2025年6月15日

分析平台:

[摸瓜APK反编译平台](#)

文件信息

文件名: TGKJ.apk

文件大小: 40.65MB

MD5值: a05ed82d7cc85af792ed53652f6d8850

SHA1值: 373e77c1f1f22336a820c8e72c6513ea24158958

SHA256值: efd4c4ab86247870c3c123eb9ce8c22e3f2013494842f21f4d5efa78c5caea32

APP 信息

App名称: TG

包名: tCgzvUhmcW.axmsdn.swjpfjs.slzpslgf

主活动Activity: com.dingding.tg.zgqocikActivity

安卓版本名称: 2.88.7

安卓版本: 1

域名线索

域名	服务器信息

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
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
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
opentest.bmob.cn	没有服务器地理信息.
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
www.openssl.org	IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
store.hispac.hicloud.com	IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
	IP: 221.194.162.215 所属国家: China

www.taobao.com	地区: Hebei 城市: Langfang 纬度: 39.509720 经度: 116.694717
metrics1.data.hicloud.com	IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
grs.dbankcloud.asia	IP: 49.4.35.251 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
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
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
app.bmob.iwyttc.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
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

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
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
h.trace.qq.com	IP: 113.56.189.246 所属国家: China 地区: Hubei 城市: Huangshi 纬度: 30.204170 经度: 115.077606
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
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
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
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
	IP: 121.36.116.8 所属国家: China

grs.dbankcloud.cn	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
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
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
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
open.weixin.qq.com	IP: 140.207.176.25 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
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
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

goo.gl	IP: 142.250.217.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
m.toutiao.com	IP: 123.125.216.197 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
cn.register.xmpush.xiaomi.com	IP: 123.125.102.39 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
open3.bmob.cn	没有服务器地理信息.
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

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
www.bjtime.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
imtest6.netease.im	没有服务器地理信息.
ip-api.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
dr.netease.im	IP: 220.197.34.83 所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
ns.adobe.com	没有服务器地理信息.
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
www.jd.com	IP: 60.9.5.200 所属国家: China 地区: Hebei 城市: Hengshui 纬度: 37.732220 经度: 115.701157

grs.dbankcloud.eu	没有服务器地理信息.
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
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
wannos.127.net	IP: 45.127.129.21 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
android.bugly.qq.com	IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
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
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
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: 220.197.34.72

roomserver.netease.im	所属国家: China 地区: Sichuan 城市: Leshan 纬度: 29.562281 经度: 103.763863
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
schemas.android.com	没有服务器地理信息.
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
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
appgallery.cloud.huawei.com	IP: 121.36.118.136 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
metrics2.data.hicloud.com	IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel 纬度: 54.321358 经度: 10.134532
	IP: 111.206.174.194 所属国家: China 地区: Beijing

resolver.msg.xiaomi.net	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
grs.dbankcloud.com	IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
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
api.weixin.qq.com	IP: 116.128.170.42 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
p.bmob.cn	没有服务器地理信息.
nrtc.netease.im	IP: 47.96.10.89 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
xmlpull.org	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
file.bmob.cn	没有服务器地理信息.
	IP: 151.101.2.132 所属国家: United States of America

xml.apache.org	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
play.google.com	IP: 142.250.69.206 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
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
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
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

 URL线索

URL信息	Url所在文件
http://www.bouncycastle.org)	UVyLauNk4bVouDAnlOly/SwgVajLSplvrSoSmOoZf/C3052.java
http://...	UVyLauNk4bVouDAnlOly/DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/XxX49JcE832HnKCSfUzS/C1704.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/AbstractC1635.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/AbstractC1612.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/AbstractC1622.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/AbstractC1646.java

https://github.com/ReactiveX/RxJava/wiki/Plugins	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/AbstractC1623.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/IdEozve3ONcALXmuhi36/C1529.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	DOo4KuiNiSZI6SMZkrw6/XxX49JcE832HnKCSfUzS/IdEozve3ONcALXmuhi36/C1531.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://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
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.jd.com/	com/netease/nim/uikit/business/session/activity/fragment/JingFragment.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.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://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/adjs	com/tencent/smtt/utlis/n.java
http://log.tbs.qq.com/ajax?c=ucfu&k=	com/tencent/smtt/utlis/n.java
http://soft.tbs.imtt.qq.com/17421/tbs_res_imtt_tbs_DebugPlugin_DebugPlugin.tbs	com/tencent/smtt/utlis/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×tamp=%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
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://ns.adobe.com/xap/1.0/\u0000	jpVzdBuZjl8brvVskoH/a2TIGGLFncC9YpCegIP6/jpVzdBuZjl8brvVskoH/C5571.java
http://schemas.android.com/apk/res/android	jpVzdBuZjl8brvVskoH/wQdxKi9IwuyiBHJb1rs/w781skZDHvFFjQR4N8rj/G8vktjvSpQLWu2KDCoIH/C7082.java
http://127.0.0.1	w781skZDHvFFjQR4N8rj/A9OZyv2npjy5HdSUaYhv/XxX49JcE832HnKCSfUzS/XxX49JcE832HnKCSfUzS/w781skZDHvFFjQR4N8rj/AbstractC7264.java
https://h.trace.qq.com/kv	w781skZDHvFFjQR4N8rj/XyPS1kw73pLHdk7HLQoL/XxX49JcE832HnKCSfUzS/w781skZDHvFFjQR4N8rj/C8058.java
https://astat.bugly.qcloud.com/rqd/async	w781skZDHvFFjQR4N8rj/XyPS1kw73pLHdk7HLQoL/XxX49JcE832HnKCSfUzS/w781skZDHvFFjQR4N8rj/C8097.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	w781skZDHvFFjQR4N8rj/XyPS1kw73pLHdk7HLQoL/XxX49JcE832HnKCSfUzS/w781skZDHvFFjQR4N8rj/C8097.java
http://m.toutiao.com	w781skZDHvFFjQR4N8rj/ZW5qqgC6jXgDYxUn6gfb/XxX49JcE832HnKCSfUzS/C8618.java
http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red	w781skZDHvFFjQR4N8rj/ZW5qqgC6jXgDYxUn6gfb/XxX49JcE832HnKCSfUzS/rUYLSzC49LqQxh2xGDc5/XxX49JcE832HnKCSfUzS/InterfaceC8543.java
http://xml.apache.org/xslt	w781skZDHvFFjQR4N8rj/dMI5CNQC6yGrnw4gPKKS/XxX49JcE832HnKCSfUzS/C8744.java
http://xml.apache.org/xslt	w781skZDHvFFjQR4N8rj/jhUx1xQH3BePdNfh74Yt/XxX49JcE832HnKCSfUzS/C9059.java
http://www.bjtime.cn	w781skZDHvFFjQR4N8rj/jpVzdBuZjl8brvVskoH/XxX49JcE832HnKCSfUzS/FTPjyPdKXxMFbJuVsQV5/C9090.java
http://www.baidu.com	w781skZDHvFFjQR4N8rj/jpVzdBuZjl8brvVskoH/XxX49JcE832HnKCSfUzS/FTPjyPdKXxMFbJuVsQV5/C9090.java
http://www.taobao.com	w781skZDHvFFjQR4N8rj/jpVzdBuZjl8brvVskoH/XxX49JcE832HnKCSfUzS/FTPjyPdKXxMFbJuVsQV5/C9090.java
http://www.ntsc.ac.cn	w781skZDHvFFjQR4N8rj/jpVzdBuZjl8brvVskoH/XxX49JcE832HnKCSfUzS/FTPjyPdKXxMFbJuVsQV5/C9090.java
http://www.time.ac.cn/	w781skZDHvFFjQR4N8rj/jpVzdBuZjl8brvVskoH/XxX49JcE832HnKCSfUzS/FTPjyPdKXxMFbJuVsQV5/C9090.java
https://play.google.com/store/apps/details?id=	w781skZDHvFFjQR4N8rj/urR4UTMVyoB9ylGITOPI/XxX49JcE832HnKCSfUzS/ZW5qqgC6jXgDYxUn6gfb/C9593.java
https://play.google.com/store	摸瓜V1引擎
https://appgallery.cloud.huawei.com/app/	摸瓜V1引擎
https://play.google.com/store/apps/details?id=	摸瓜V1引擎
https://appgallery.cloud.huawei.com	摸瓜V1引擎
https://store.hispac.hicloud.com/hwmarket/api/	摸瓜V1引擎
https://grs.dbankcloud.com	摸瓜V2引擎
https://grs.dbankcloud.cn	摸瓜V2引擎

https://grs.dbankcloud.eu	摸瓜V2引擎
https://grs.dbankcloud.asia	摸瓜V2引擎
https://metrics1.data.hicloud.com:6447	摸瓜V2引擎
https://metrics-dra.dt.hicloud.com:6447	摸瓜V2引擎
https://metrics2.data.hicloud.com:6447	摸瓜V2引擎
https://metrics5.data.hicloud.com:6447	摸瓜V2引擎
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libnrtc_sdk.so
https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/librwzrxcpimj.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/librts_network.so

 邮箱线索

邮箱地址	所在文件
rubin@rubindemacbook-pro.local	com/netease/yunxin/nos/sdk/NosFacade.java
rubin@rubindemacbook-pro.local	com/netease/yunxin/report/sdk/ReportManager.java
hyy@gmail.com 732662@sina.com hyy@139.com hyy-123@163.com hyy12@qq.com hyy@sohu.com hyy@hotmail.com hyy@189.cn	w781skZDHvFFjQR4N8rj/urR4UTMVyoB9ylGITOPi/XxX49JcE832HnKCSfUzS/dMI5CNQC6yGrnw4gPKKS/C9614.java

 手机线索

手机号	所在文件
15095675534	UVyLauNk4bVouDAnlOly/SwgVajLSplvrSoSmOoZf/jpVzdBuZjl8brvVskcoH/yehG3hhSzgY1GzHhUTHF/C2936.java
17179869184	UVyLauNk4bVouDAnlOly/SwgVajLSplvrSoSmOoZf/ZW5qqgC6jXgDYxUn6gfb/SwgVajLSplvrSoSmOoZf/XxX49JcE832HnKCSfUzS/C2306.java

17179869183	UVyLauNk4bVouDAnlOly/SwgVajLSplvrSoSmOoZf/ZW5qqgC6JXgDYxUn6gfb/SwgVajLSplvrSoSmOoZf/XxX49JcE832HnKCSfUzS/C2306.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: True
v2 签名: True
v3 签名: True
找到 1 个唯一证书
主题: C=gDSgkVpy, ST=aSkUtQCB, L=BRSPHPEI, O=cyTiKHYA, OU=LKgcQkLP, CN=wwFLrsXn
签名算法: rsassa_pkcs1v15
有效期自: 2025-04-23 02:18:55+00:00
有效期至: 2035-04-21 02:18:55+00:00
发行人: C=gDSgkVpy, ST=aSkUtQCB, L=BRSPHPEI, O=cyTiKHYA, OU=LKgcQkLP, CN=wwFLrsXn
序列号: 0x26cec808aae6e840
哈希算法: sha256
md5值: 78c7b344c2f82a5fa13d67e05b6a503c
sha1值: dfbb2a0b6265230a5f0423802076cf303d773f76
sha256值: 33adc17ec31597aadcb3910e96362ce34fbd01c9d57ad773e0647ae735722079
sha512值: 7a6c4cfc0ed23be775026ffc5966973fd970bf427c617d764cfc427d2728767ccb87c36b374c3b7c7879e1b8b14adfb3065869a254575103b8c1a9a6cdf94f1a
公钥算法: rsa
密钥长度: 2048
指纹: 80b38d8f1e6b641a81360c6ed084e29670591b5624490ec222626ca42af74e89

🔑 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_confim_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
	正	访问额外的	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

android.permission.ACCESS_LOCATION_EXTRA_COMMANDS	常	位置提供程序命令	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。
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.permission.MIPUSH_RECEIVE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.permission.C2D_MESSAGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.coloros.mcs.permission.RECIEVE_MCS_MESSAGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.heytao.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
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.meizu.flyme.push.permission.RECEIVE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.push.permission.MESSAGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_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.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.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
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.sec.android.provider.badge.permission.READ	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.sec.android.provider.badge.permission.WRITE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.htc.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference

tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.htc.launcher.permission.UPDATE_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.sonyericsson.home.permission.BROADCAST_BADGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.sonymobile.home.permission.PROVIDER_INSERT_BADGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.anddoes.launcher.permission.UPDATE_COUNT	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.majeur.launcher.permission.UPDATE_BADGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.huawei.android.launcher.permission.CHANGE_BADGE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.huawei.android.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.huawei.android.launcher.permission.WRITE_SETTINGS	未知	Unknown 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
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.oppo.launcher.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_com.oppo.launcher.permission.WRITE_SETTINGS	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_me.everything.badger.permission.BADGE_COUNT_READ	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_me.everything.badger.permission.BADGE_COUNT_WRITE	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.permission.PROCESS_PUSH_MSG	未知	Unknown permission	Unknown permission from android reference
tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU.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。

tCgzvUhmcW.lzWqv.duAxrVGdSm.qppmkDiSUXOesU_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。