Evaluation Warning: The document was created with Spire.Doc for Python.

**博文（ 1.1.3版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 博文 |
| 版本 | 1.1.3 |
| 包名 | com.vexqqn.azczhwhx |
| 域名线索 | 77条 |
| URL线索 | 78条 |
| APP图标 |  |
| 分析日期 | 2025年7月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 5\_base.apk |
| 文件大小 | 40.08MB |
| MD5值 | 6b8acf383b76c3c255836921ac7a68fa |
| SHA1值 | c47d53f32c4916474dbff5df9c920be09d82f412 |
| SHA256值 | 2691ea874526a0294f9387ffe55db171c3be1b12c0baf42e1d5f22c737586a21 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| 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 |

## **4. 线索情况**

### **4.1 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 |
| imtest4.netease.im | IP: 59.111.241.163  所属国家: China  地区: Guangdong  城市: Guangzhou |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| nosup-hz1.127.net | IP: 45.127.129.8  所属国家: China  地区: Guangdong  城市: Guangzhou |
| metrics1.data.hicloud.com | IP: 111.202.16.252  所属国家: China  地区: Beijing  城市: Beijing |
| 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 |
| www.ntsc.ac.cn | IP: 159.226.242.43  所属国家: China  地区: Beijing  城市: Beijing |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| store.hispace.hicloud.com | IP: 123.249.62.130  所属国家: China  地区: Guangdong  城市: Guangzhou |
| 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 |
| pms.mb.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| 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 |
| grs.dbankcloud.cn | IP: 49.4.40.185  所属国家: China  地区: Guangdong  城市: Guangzhou |
| m0.api.upyun.com | IP: 218.60.175.252  所属国家: China  地区: Liaoning  城市: Dandong |
| cfg.imtt.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| fr.register.xmpush.global.xiaomi.com | IP: 98.64.182.160  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| 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 |
| ip-api.com | IP: 208.95.112.1  所属国家: United States of America  地区: North Carolina  城市: Skyland |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.jivesoftware.com | IP: 23.235.209.143  所属国家: United States of America  地区: Virginia  城市: Virginia Beach |
| mdc.html5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| p0.api.upyun.com | IP: 101.251.144.15  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dr.netease.im | IP: 101.71.139.136  所属国家: China  地区: Zhejiang  城市: Ningbo |
| 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 |
| roomserver.netease.im | IP: 47.96.190.103  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| goo.gl | IP: 142.251.43.14  所属国家: United States of America  地区: California  城市: Mountain View |
| imtest.netease.im | IP: 59.111.209.232  所属国家: China  地区: Guangdong  城市: Guangzhou |
| www.bjtime.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| wup.imtt.qq.com | IP: 125.39.104.63  所属国家: China  地区: Tianjin  城市: Tianjin |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| api-push.meizu.com | IP: 221.5.93.66  所属国家: China  地区: Guangdong  城市: Foshan |
| grs.dbankcloud.asia | IP: 121.36.116.8  所属国家: China  地区: Beijing  城市: Beijing |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.tbs.qq.com | IP: 124.95.224.248  所属国家: China  地区: Liaoning  城市: Shenyang |
| api-push.in.meizu.com | IP: 206.161.233.191  所属国家: United States of America  地区: Virginia  城市: Herndon |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| open.weixin.qq.com | IP: 223.167.82.219  所属国家: China  地区: Shanghai  城市: Shanghai |
| m.toutiao.com | IP: 182.40.61.216  所属国家: China  地区: Shandong  城市: Qingdao |
| www.jd.com | IP: 123.6.77.65  所属国家: China  地区: Henan  城市: Zhengzhou |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| api.weixin.qq.com | IP: 116.128.184.169  所属国家: China  地区: Shanghai  城市: Shanghai |
| resolver.msg.global.xiaomi.net | IP: 8.219.74.181  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.openssl.org | IP: 34.36.58.177  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| io.codenow.cn | IP: 106.75.70.127  所属国家: China  地区: Shanghai  城市: Shanghai |
| astat.bugly.qcloud.com | IP: 119.28.121.133  所属国家: Singapore  地区: Singapore  城市: Singapore |
| 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 |
| 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 |
| www.taobao.com | IP: 61.182.130.193  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| www.baidu.com | IP: 110.242.68.3  所属国家: China  地区: Hebei  城市: Baoding |
| grs.dbankcloud.com | IP: 113.201.107.54  所属国家: China  地区: Shaanxi  城市: Baoji |
| qyqa.netease.com | IP: 59.111.96.241  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.bouncycastle.org | IP: 203.32.61.103  所属国家: Australia  地区: Victoria  城市: Drouin |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| resolver.msg.xiaomi.net | IP: 111.202.1.252  所属国家: China  地区: Beijing  城市: Beijing |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| maps.google.cn | IP: 114.250.65.34  所属国家: China  地区: Beijing  城市: Beijing |
| metrics5.data.hicloud.com | IP: 159.138.203.215  所属国家: Russian Federation  地区: Sverdlovskaya oblast'  城市: Yekaterinburg |
| android.bugly.qq.com | IP: 124.95.225.146  所属国家: China  地区: Liaoning  城市: Shenyang |
| v0.api.upyun.com | IP: 218.60.175.252  所属国家: China  地区: Liaoning  城市: Dandong |
| norma-external-collect.meizu.com | IP: 183.60.176.112  所属国家: China  地区: Guangdong  城市: Guangzhou |
| idmb.register.xmpush.global.xiaomi.com | IP: 20.219.205.9  所属国家: India  地区: Maharashtra  城市: Pune |
| 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 |
| cn.register.xmpush.xiaomi.com | IP: 111.202.1.240  所属国家: China  地区: Beijing  城市: Beijing |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100  所属国家: Singapore  地区: Singapore  城市: Singapore |
| appgallery.cloud.huawei.com | IP: 49.4.35.16  所属国家: China  地区: Guangdong  城市: Guangzhou |
| metrics2.data.hicloud.com | IP: 80.158.38.48  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| www.time.ac.cn | IP: 210.72.145.8  所属国家: China  地区: Beijing  城市: Beijing |
| 59.111.110.241 | IP: 59.111.110.241  所属国家: China  地区: Zhejiang  城市: Hangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | YTSQe1ys7zUTWm1W5F4b/tF2eNlTcjQ8TXD7qsjsG/ckNIwYDypKyM5FPmGZ4t/gjCiE3gxDZbFjPTriaBh/C1338.java |
| http://127.0.0.1 | ckNIwYDypKyM5FPmGZ4t/PYxA7RJTP4IfhefMfaNc/gl38SVNG2KZpFvuqFleF/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/AbstractC2821.java |
| http://xml.apache.org/xslt | ckNIwYDypKyM5FPmGZ4t/YwczgpkQgURXBp9MKACf/gl38SVNG2KZpFvuqFleF/C2865.java |
| http://www.bjtime.cn | ckNIwYDypKyM5FPmGZ4t/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzlKH2fgvN9gMzn/C2886.java |
| http://www.baidu.com | ckNIwYDypKyM5FPmGZ4t/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzlKH2fgvN9gMzn/C2886.java |
| http://www.taobao.com | ckNIwYDypKyM5FPmGZ4t/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzlKH2fgvN9gMzn/C2886.java |
| http://www.ntsc.ac.cn | ckNIwYDypKyM5FPmGZ4t/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzlKH2fgvN9gMzn/C2886.java |
| http://www.time.ac.cn/ | ckNIwYDypKyM5FPmGZ4t/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/nWDshVzlKH2fgvN9gMzn/C2886.java |
| http://xml.apache.org/xslt | ckNIwYDypKyM5FPmGZ4t/nFdI4qFibYdUYjry1rCD/gl38SVNG2KZpFvuqFleF/C3739.java |
| https://play.google.com/store/apps/details?id= | ckNIwYDypKyM5FPmGZ4t/oEIoUTRrYHY9pXT3mUdM/gl38SVNG2KZpFvuqFleF/YwczgpkQgURXBp9MKACf/C3932.java |
| https://astat.bugly.qcloud.com/rqd/async | ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21fIwlMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4157.java |
| https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async | ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21fIwlMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4157.java |
| https://h.trace.qq.com/kv | ckNIwYDypKyM5FPmGZ4t/oqj7JUyW21fIwlMMGuTn/gl38SVNG2KZpFvuqFleF/ckNIwYDypKyM5FPmGZ4t/C4103.java |
| http://m.toutiao.com | ckNIwYDypKyM5FPmGZ4t/wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/C4690.java |
| http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red | ckNIwYDypKyM5FPmGZ4t/wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/oEIoUTRrYHY9pXT3mUdM/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=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 |
| 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&timestamp=%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/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 |
| 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) | rb9RtYti3qujsUEAIFON/aOPC4z5PzTttcKRXizg9/C7549.java |
| http://... | rb9RtYti3qujsUEAIFON/wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/gl38SVNG2KZpFvuqFleF/C7641.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9318.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9336.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9350.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9338.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/AbstractC9342.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | wDHeulSM4rslLEyqcmiC/gl38SVNG2KZpFvuqFleF/KJCeBaZNoHMe52vPYFMW/C7731.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | wDHeulSM4rslLEyqcmiC/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/libsmcderxrpocbv.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 |

### **4.3 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 |

### **4.4 手机号线索**

| 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/YwczgpkQgURXBp9MKACf/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/C6931.java |
| 17179869183 | rb9RtYti3qujsUEAIFON/aOPC4z5PzTttcKRXizg9/YwczgpkQgURXBp9MKACf/aOPC4z5PzTttcKRXizg9/gl38SVNG2KZpFvuqFleF/C6931.java |

## **5. 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=zuxIQolF 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=zuxIQolF 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**

## **6. 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" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.kxLWDkDWLnalEI.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 |

## **10. 应用内通信**

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