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

**曹妃甸核酸检测平台（ 1.0.6-6p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 | 曹妃甸核酸检测平台 |
| 版本 | 1.0.6-6p |
| 包名 | com.hbstss.cfdhsjyfwpt |
| 域名线索 | 99条 |
| URL线索 | 138条 |
| APP图标 |  |
| 分析日期 | 2025年7月1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 | REL\_Doctor\_1.0.6-6p-2022.05.18.apk |
| 文件大小 | 25.2MB |
| MD5值 | 87e86dde00a2a5ec7a4fe4faa3ace5ed |
| SHA1值 | 59d740cd3580f41e08fd4cf0d5e6d2e8ccb992a1 |
| SHA256值 | 197dd0b44badb8ee0c47329e92b339e975ec214fc590dbe13f2af8540df9862d |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 曹妃甸核酸检测平台 |
| 包名 | com.hbstss.cfdhsjyfwpt |
| 主活动Activity | com.health.doctor.start.LoadingActivity |
| 安卓版本名称 | 1.0.6-6p |
| 安卓版本 | 6 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| 101.231.114.224 | IP: 101.231.114.224  所属国家: China  地区: Shanghai  城市: Shanghai |
| sv0.map.bdimg.com | IP: 111.206.209.186  所属国家: China  地区: Beijing  城市: Beijing |
| roomserver.netease.im | IP: 59.111.248.65  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 |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| itsdata.map.baidu.com | IP: 111.206.209.180  所属国家: China  地区: Beijing  城市: Beijing |
| sissi.pingxx.com | IP: 118.31.129.67  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umeng.com | IP: 223.109.148.176  所属国家: China  地区: Beijing  城市: Beijing |
| wappaygw.alipay.com | IP: 124.239.239.237  所属国家: China  地区: Hebei  城市: Langfang |
| imtest.netease.im | IP: 59.111.241.163  所属国家: China  地区: Guangdong  城市: Guangzhou |
| goo.gl | IP: 172.217.160.78  所属国家: United States of America  地区: California  城市: Mountain View |
| myipad.dccnet.com.cn | IP: 114.255.225.27  所属国家: China  地区: Beijing  城市: Beijing |
| mta.oa.com | IP: 193.123.33.15  所属国家: Netherlands  地区: Noord-Holland  城市: Amsterdam |
| mywap2.dccnet.com.cn | IP: 60.247.121.179  所属国家: China  地区: Beijing  城市: Beijing |
| sv.map.baidu.com | IP: 111.206.209.186  所属国家: China  地区: Beijing  城市: Beijing |
| 101.231.204.80 | IP: 101.231.204.80  所属国家: China  地区: Shanghai  城市: Shanghai |
| www.163.com | IP: 61.136.232.157  所属国家: China  地区: Hubei  城市: Shiyan |
| www.w3.org | IP: 128.30.52.100  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| service.weibo.com | IP: 49.7.40.132  所属国家: China  地区: Beijing  城市: Beijing |
| 140.207.168.45 | IP: 140.207.168.45  所属国家: China  地区: Shanghai  城市: Shanghai |
| statistic.live.126.net | IP: 183.136.182.46  所属国家: China  地区: Guangdong  城市: Guangzhou |
| lbs.netease.im | IP: 59.111.211.9  所属国家: China  地区: Guangdong  城市: Guangzhou |
| cgi.connect.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobiletest.yeepay.com | IP: 58.83.141.73  所属国家: China  地区: Beijing  城市: Beijing |
| sdk.open.inc2.igexin.com | 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 |
| jabber.org | IP: 208.68.163.218  所属国家: United States of America  地区: Iowa  城市: Monticello |
| api.weibo.com | IP: 49.7.37.118  所属国家: China  地区: Beijing  城市: Beijing |
| api.weixin.qq.com | IP: 81.69.216.43  所属国家: China  地区: Beijing  城市: Beijing |
| v.map.baidu.com | IP: 111.206.209.185  所属国家: China  地区: Beijing  城市: Beijing |
| appsupport.qq.com | IP: 175.27.9.43  所属国家: China  地区: Beijing  城市: Beijing |
| api.map.baidu.com | IP: 111.206.209.166  所属国家: China  地区: Beijing  城市: Beijing |
| 101.231.114.238 | IP: 101.231.114.238  所属国家: China  地区: Shanghai  城市: Shanghai |
| plbslog.umeng.com | IP: 36.156.202.73  所属国家: China  地区: Beijing  城市: Beijing |
| jivesoftware.org | IP: 216.146.46.11  所属国家: United States of America  地区: California  城市: Belmont |
| pslog.umeng.com | IP: 59.82.29.163  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| imtest.91taogu.com | IP: 121.42.24.173  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| aaid.umeng.com | IP: 218.91.197.67  所属国家: China  地区: Jiangsu  城市: Nantong |
| long.open.weixin.qq.com | IP: 109.244.217.35  所属国家: China  地区: Beijing  城市: Beijing |
| sdk.open.amp.igexin.com | IP: 183.134.98.71  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pingma.qq.com | IP: 119.45.78.184  所属国家: China  地区: Beijing  城市: Beijing |
| mobile.unionpay.com | 没有服务器地理信息. |
| mcgw.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| media.weibo.cn | IP: 49.7.40.144  所属国家: China  地区: Beijing  城市: Beijing |
| mclient.alipay.com | IP: 124.239.239.236  所属国家: China  地区: Hebei  城市: Langfang |
| wspeed.qq.com | 没有服务器地理信息. |
| www.igniterealtime.org | IP: 52.58.216.59  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| master.91taogu.com | IP: 47.105.86.31  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobilegw.alipay.com | IP: 203.209.247.65  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.jivesoftware.com | IP: 35.238.7.255  所属国家: United States of America  地区: Iowa  城市: Council Bluffs |
| test.91taogu.com | IP: 121.42.24.173  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wp.map.baidu.com | IP: 111.206.209.185  所属国家: China  地区: Beijing  城市: Beijing |
| its.map.baidu.com | IP: 153.37.235.49  所属国家: China  地区: Jiangsu  城市: Suzhou |
| alogsus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Beijing  城市: Beijing |
| aip.baidubce.com | IP: 111.206.210.12  所属国家: China  地区: Beijing  城市: Beijing |
| im.91taogu.com | IP: 121.42.29.230  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m.alipay.com | IP: 203.209.245.74  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| 120.204.69.182 | IP: 120.204.69.182  所属国家: China  地区: Shanghai  城市: Shanghai |
| verify.baidubce.com | IP: 110.242.69.180  所属国家: China  地区: Hebei  城市: Baoding |
| mywap2.icbc.com.cn | IP: 123.127.121.51  所属国家: China  地区: Hainan  城市: Donglu |
| ok.yeepay.com | IP: 101.36.145.90  所属国家: China  地区: Beijing  城市: Beijing |
| 202.101.25.178 | IP: 202.101.25.178  所属国家: China  地区: Shanghai  城市: Shanghai |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| h5.m.taobao.com | IP: 220.181.135.232  所属国家: China  地区: Beijing  城市: Beijing |
| mta.qq.com | IP: 61.54.7.126  所属国家: China  地区: Henan  城市: Anyang |
| open.weixin.qq.com | IP: 175.24.209.30  所属国家: China  地区: Beijing  城市: Beijing |
| developer.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ibsbjstar.ccb.com.cn | IP: 114.251.28.2  所属国家: China  地区: Beijing  城市: Beijing |
| health91.oss-cn-qingdao.aliyuncs.com | IP: 47.104.36.39  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.polites.com | IP: 192.0.78.25  所属国家: United States of America  地区: California  城市: San Francisco |
| ulogs.umengcloud.com | IP: 223.109.148.141  所属国家: China  地区: Beijing  城市: Beijing |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| etherx.jabber.org | IP: 208.68.163.210  所属国家: United States of America  地区: Iowa  城市: Monticello |
| 101.231.114.217 | IP: 101.231.114.217  所属国家: China  地区: Shanghai  城市: Shanghai |
| fe-beta1.91taogu.com | IP: 114.215.131.191  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apia.91taogu.com | IP: 47.105.86.31  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.91taogu.com | IP: 47.105.86.31  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| nosup-hz1.127.net | IP: 45.127.129.16  所属国家: China  地区: Guangdong  城市: Guangzhou |
| alogus.umeng.com | IP: 223.109.148.178  所属国家: China  地区: Beijing  城市: Beijing |
| imtest6.netease.im | 没有服务器地理信息. |
| xmlpull.org | IP: 74.50.61.58  所属国家: United States of America  地区: Texas  城市: Dallas |
| open.weibo.cn | IP: 49.7.37.118  所属国家: China  地区: Beijing  城市: Beijing |
| maps.google.com | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| daup.map.baidu.com | IP: 110.242.69.98  所属国家: China  地区: Hebei  城市: Baoding |
| www.jivesoftware.org | IP: 216.146.46.11  所属国家: United States of America  地区: California  城市: Belmont |
| sdk.open.phone.igexin.com | IP: 183.131.7.116  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| test2.91taogu.com | IP: 121.42.194.84  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| dr.netease.im | IP: 59.111.238.11  所属国家: China  地区: Guangdong  城市: Guangzhou |
| master-test.91taogu.com | IP: 121.42.24.173  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| m.weibo.cn | IP: 218.30.115.44  所属国家: China  地区: Beijing  城市: Beijing |
| loc.map.baidu.com | IP: 111.206.209.175  所属国家: China  地区: Beijing  城市: Beijing |
| client.map.baidu.com | IP: 111.206.209.120  所属国家: China  地区: Beijing  城市: Beijing |
| www.openssl.org | IP: 104.100.76.250  所属国家: United States of America  地区: California  城市: San Jose |
| nrtc.netease.im | IP: 59.111.248.65  所属国家: China  地区: Guangdong  城市: Guangzhou |
| app.91taogu.com | IP: 47.104.203.83  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 172.17.236.169 | IP: 172.17.236.169  所属国家: -  地区: -  城市: - |
| schemas.android.com | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobile.unionpay.com/getclient?platform=android&type=securepayplugin | com/unionpay/C0441a.java |
| http://140.207.168.45/g/d | com/unionpay/c/I.java |
| https://api.weixin.qq.com/sns/oauth2/access\_token?appid= | com/toogoo/appbase/share/AbstractWXEntryActivity.java |
| http://www.w3.org/2000/svg | com/toogoo/appbase/e/a/c.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/app/PayTask.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/util/n.java |
| http://m.alipay.com/?action=h5quit | com/alipay/sdk/util/o.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://pslog.umeng.com | com/umeng/commonsdk/vchannel/a.java |
| https://pslog.umeng.com/ | com/umeng/commonsdk/vchannel/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://alogsus.umeng.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://ulogs.umengcloud.com | com/umeng/commonsdk/statistics/UMServerURL.java |
| https://developer.umeng.com/docs/66632/detail/ | com/umeng/commonsdk/debug/UMLogUtils.java |
| https://plbslog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ulogs.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://ouplog.umeng.com | com/umeng/commonsdk/stateless/a.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/i.java |
| https://aaid.umeng.com/api/postZdata | com/umeng/umzid/ZIDManager.java |
| https://aaid.umeng.com/api/updateZdata | com/umeng/umzid/ZIDManager.java |
| http://jabber.org/protocol/disco#info | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/nick+notify | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/xhtml-im | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/muc | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/si/profile/file-transfer | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/si | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/ibb | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/feature-neg | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/muc#user | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/disco#items | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/offline | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/muc#admin | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/muc#owner | com/xbcx/im/IMSystem.java |
| http://jabber.org/protocol/chatstates | com/xbcx/im/IMSystem.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | com/xbcx/im/p.java |
| http://jabber.org/protocol/muc#user | com/xbcx/im/XIMSystem.java |
| http://maps.google.com/maps/api/staticmap?center=%f,%f&zoom=%d&size=%dx%d&maptype=roadmap&markers=color:red%%7Clabel:%%7C%f,%f&sensor=false&language=zh-Hans | com/xbcx/core/XApplication.java |
| http://test2.91taogu.com/api | com/xbcx/core/n.java |
| https://health91.oss-cn-qingdao.aliyuncs.com/ | com/yht/util/z.java |
| https://apia.91taogu.com | com/yht/util/HostUtils.java |
| https://app.91taogu.com | com/yht/util/HostUtils.java |
| http://im.91taogu.com | com/yht/util/HostUtils.java |
| https://master-test.91taogu.com/ | com/yht/util/HostUtils.java |
| https://master.91taogu.com/ | com/yht/util/HostUtils.java |
| https://fe-beta1.91taogu.com | com/yht/util/HostUtils.java |
| https://test.91taogu.com | com/yht/util/HostUtils.java |
| https://api.91taogu.com | com/yht/util/HostUtils.java |
| http://api.91taogu.com | com/yht/util/HostUtils.java |
| https://im.91taogu.com | com/yht/util/HostUtils.java |
| http://imtest.91taogu.com:4080 | com/yht/util/HostUtils.java |
| http://im.91taogu.com/SDKapi | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_department\_getlist | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_user\_info | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_start\_login | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_start\_reg | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_user\_search | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_user\_setinfo | com/example/xbcxim\_demo/app/HttpUrl.java |
| http://im.91taogu.com/SDKapi/index.php?a=\_upfile | com/example/xbcxim\_demo/app/HttpUrl.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.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/d.java |
| http://appsupport.qq.com/cgi-bin/appstage/mstats\_batch\_report | com/tencent/open/b/k.java |
| http://wspeed.qq.com/w.cgi | com/tencent/open/b/j.java |
| http://cgi.connect.qq.com/qqconnectopen/openapi/policy\_conf | com/tencent/open/utils/c.java |
| http://mta.qq.com/ | com/tencent/wxop/stat/e.java |
| http://mta.oa.com/ | com/tencent/wxop/stat/e.java |
| http://pingma.qq.com:80/mstat/report | com/tencent/wxop/stat/c.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/bankcard? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/idcard? | com/baidu/ocr/sdk/OCR.java |
| https://verify.baidubce.com/verify/1.0/token/sk?sdkVersion=1\_4\_4 | com/baidu/ocr/sdk/OCR.java |
| https://verify.baidubce.com/verify/1.0/token/bin?sdkVersion=1\_4\_4 | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate\_basic? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/accurate? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/business\_card? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/business\_license? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/solution/v1/iocr/recognise? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/driving\_license? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_basic? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general\_enhanced? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/general? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/webimage? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/handwriting? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/license\_plate? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/lottery? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/numbers? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/passport? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/qrcode? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/receipt? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/vat\_invoice? | com/baidu/ocr/sdk/OCR.java |
| https://aip.baidubce.com/rest/2.0/ocr/v1/vehicle\_license? | com/baidu/ocr/sdk/OCR.java |
| https://verify.baidubce.com/verify/1.0/sdk/report | com/baidu/ocr/sdk/utils/CrashReporterHandler.java |
| https://itsdata.map.baidu.com/long-conn-gps/sdk.php | com/baidu/location/b/f.java |
| http://loc.map.baidu.com/cc.php | com/baidu/location/b/d.java |
| http://loc.map.baidu.com/user\_err.php | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/oqur.php | com/baidu/location/e/k.java |
| https://loc.map.baidu.com/tcu.php | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/rtbu.php | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/iofd.php | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/wloc | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/sdk.php | com/baidu/location/e/k.java |
| http://loc.map.baidu.com/sdk\_ep.php | com/baidu/location/e/k.java |
| https://loc.map.baidu.com/sdk.php | com/baidu/location/e/k.java |
| https://daup.map.baidu.com/cltr/rcvr | com/baidu/location/e/k.java |
| https://api.map.baidu.com/sdkcs/verify | com/baidu/lbsapi/auth/LBSAuthManager.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/sdk/PushBuildConfig.java |
| http://sdk.open.inc2.igexin.com/api.php | com/igexin/getuiext/data/Consts.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/getuiext/data/Consts.java |
| http://sdk.open.phone.igexin.com/api.php?format=json&t=1 | com/igexin/getuiext/service/i.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/push/a/k.java |
| http://sdk.open.phone.igexin.com:8003/api.php | com/igexin/push/a/k.java |
| http://sdk.open.phone.igexin.com/api.php | com/igexin/push/core/g.java |
| http://sdk.open.amp.igexin.com/api.htm | com/igexin/push/core/a/f.java |
| http://m.weibo.cn/u/ | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://media.weibo.cn/article? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/comment? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/ | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/index/router? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| https://m.weibo.cn/p/100103type=1& | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://m.weibo.cn/mblog? | com/sina/weibo/sdk/web/WeiboPageUtils.java |
| http://service.weibo.com/share/mobilesdk.php | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java |
| http://service.weibo.com/share/mobilesdk\_uppic.php | com/sina/weibo/sdk/web/param/ShareWebViewRequestParam.java |
| https://api.weibo.com/oauth2/access\_token | com/sina/weibo/sdk/auth/AccessTokenKeeper.java |
| https://open.weibo.cn/oauth2/authorize? | com/sina/weibo/sdk/auth/BaseSsoHandler.java |
| https://api.weibo.com/oauth2/getaid.json | com/sina/weibo/sdk/utils/AidTask4Plug.java |
| https://api.weibo.com/oauth2/getaid.json | com/sina/weibo/sdk/utils/AidTask.java |
| https://api.weibo.com/2/proxy/sdk/statistic.json | com/sina/weibo/sdk/statistic/LogReport.java |
| https://nrtc.netease.im/nrtc/getChannelInfos.action | com/netease/nrtc/b.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://roomserver.netease.im/v1/sdk/command/rooms | com/netease/nrtc/engine/impl/h.java |
| http://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://goo.gl/FE5SeB | com/netease/nrtc/utility/l.java |
| https://nrtc.netease.im/nrtc/uploadSdkLog.action | com/netease/nrtc/utility/b/a.java |
| http://statistic.live.126.net/statistic/realtime/sdkinfo | com/netease/nrtc/monitor/j.java |
| http://statistic.live.126.net/statistic/realtime/sdkFunctioninfo | com/netease/nrtc/monitor/d.java |
| https://statistic.live.126.net/statics/report/common/form | com/netease/yunxin/report/sdk/ReportComponent.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 |
| 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/f/g.java |
| https://imtest.netease.im/lbs/conf.jsp | com/netease/nimlib/f/e.java |
| https://imtest.netease.im/1.gif | com/netease/nimlib/f/e.java |
| https://imtest4.netease.im/test | com/netease/nimlib/f/e.java |
| https://imtest6.netease.im:8012/ | com/netease/nimlib/f/e.java |
| https://imtest.netease.im/lbsrc/conf.jsp | com/netease/nimlib/f/e.java |
| https://lbs.netease.im/lbs/conf.jsp | com/netease/nimlib/f/e.java |
| https://dr.netease.im/1.gif | com/netease/nimlib/f/e.java |
| www.163.com | com/netease/nimlib/s/k.java |
| http://statistic.live.126.net/statics/report/common/form | com/netease/nimlib/d/f/a.java |
| http://schemas.android.com/apk/res/android | com/polites/android/GestureImageView.java |
| http://schemas.polites.com/android | com/polites/android/GestureImageView.java |
| http://sissi.pingxx.com/mock.php?ch\_id=%s&channel=%s | com/pingplusplus/android/PaymentActivity.java |
| https://ok.yeepay.com/paymobile/api/pay/request?merchantaccount=%s&encryptkey=%s&data=%s | com/pingplusplus/android/PaymentActivity.java |
| http://mobiletest.yeepay.com/paymobile/api/pay/request?merchantaccount=%s&encryptkey=%s&data=%s | com/pingplusplus/android/PaymentActivity.java |
| https://ok.yeepay.com/paymobile/query/pay/success? | com/pingplusplus/android/e.java |
| http://mobiletest.yeepay.com/paymobile/query/pay/success? | com/pingplusplus/android/e.java |
| http://xmlpull.org/v1/doc/features.html#indent-output | com/ta/utdid2/b/a/e.java |
| http://xmlpull.org/v1/doc/features.html#indent-output | com/ta/utdid2/b/a/a.java |
| https://myipad.dccnet.com.cn | com/icbc/paysdk/a/a.java |
| https://mywap2.dccnet.com.cn:447 | com/icbc/paysdk/a/a.java |
| https://mywap2.icbc.com.cn | com/icbc/paysdk/a/a.java |
| https://ibsbjstar.ccb.com.cn/ | c/b/a/a.java |
| https://ibsbjstar.ccb.com.cn/CCBIS/ccbMain? | c/b/a/c/d.java |
| https://ibsbjstar.ccb.com.cn/CCBIS/ccbMain | c/b/a/c/d.java |
| https://h5.m.taobao.com/mlapp/olist.html | c/a/b/b/a.java |
| https://mcgw.alipay.com/sdklog.do | c/a/b/e/a/c.java |
| https://mobilegw.alipay.com/mgw.htm | c/a/b/a/a.java |
| http://www.w3.org/XML/1998/namespace | asmack/com/kenai/jbosh/r.java |
| http://www.w3.org/XML/1998/namespace | asmack/com/kenai/jbosh/F.java |
| http://jabber.org/protocol/compress | asmack/org/jivesoftware/smack/PacketReader.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | asmack/org/jivesoftware/smack/PacketReader.java |
| http://jabber.org/protocol/httpbind | asmack/org/jivesoftware/smack/BOSHConnection.java |
| http://etherx.jabber.org/streams | asmack/org/jivesoftware/smack/PacketWriter.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | asmack/org/jivesoftware/smack/SmackConfiguration.java |
| http://jabber.org/protocol/compress' | asmack/org/jivesoftware/smack/XMPPConnection.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | asmack/org/jivesoftware/smack/BOSHPacketReader.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties | asmack/org/jivesoftware/smack/packet/Packet.java |
| http://www.jivesoftware.com/xmlns/xmpp/properties | asmack/org/jivesoftware/smack/util/PacketParserUtils.java |
| http://xmlpull.org/v1/doc/features.html#process-namespaces | asmack/org/jivesoftware/smack/provider/ProviderManager.java |
| http://www.igniterealtime.org/projects/smack/ | asmack/org/jivesoftware/smackx/EntityCapsManager.java |
| http://jabber.org/protocol/offline | asmack/org/jivesoftware/smackx/OfflineMessageManager.java |
| http://jabber.org/protocol/address | asmack/org/jivesoftware/smackx/MultipleRecipientManager.java |
| http://jabber.org/protocol/xhtml-im | asmack/org/jivesoftware/smackx/XHTMLManager.java |
| http://jabber.org/protocol/chatstates | asmack/org/jivesoftware/smackx/ChatStateManager.java |
| http://jabber.org/protocol/pubsub#event | asmack/org/jivesoftware/smackx/PEPManager.java |
| http://www.igniterealtime.org/projects/smack/ | asmack/org/jivesoftware/smackx/ServiceDiscoveryManager.java |
| http://jabber.org/protocol/disco#publish | asmack/org/jivesoftware/smackx/ServiceDiscoveryManager.java |
| http://jabber.org/protocol/xhtml-im | asmack/org/jivesoftware/smackx/packet/XHTMLExtension.java |
| http://jabber.org/protocol/pubsub | asmack/org/jivesoftware/smackx/packet/PEPItem.java |
| http://jabber.org/protocol/feature-neg | asmack/org/jivesoftware/smackx/packet/StreamInitiation.java |
| http://jabber.org/protocol/si/profile/file-transfer | asmack/org/jivesoftware/smackx/packet/StreamInitiation.java |
| http://jabber.org/protocol/si | asmack/org/jivesoftware/smackx/packet/StreamInitiation.java |
| http://jabber.org/protocol/offline | asmack/org/jivesoftware/smackx/packet/OfflineMessageInfo.java |
| http://jabber.org/protocol/shim | asmack/org/jivesoftware/smackx/packet/HeadersExtension.java |
| http://jabber.org/protocol/pubsub | asmack/org/jivesoftware/smackx/packet/PEPEvent.java |
| http://jabber.org/protocol/address | asmack/org/jivesoftware/smackx/packet/MultipleAddresses.java |
| http://jabber.org/protocol/muc#admin | asmack/org/jivesoftware/smackx/packet/MUCAdmin.java |
| http://jabber.org/protocol/disco#info | asmack/org/jivesoftware/smackx/packet/DiscoverInfo.java |
| http://jabber.org/protocol/ibb | asmack/org/jivesoftware/smackx/packet/IBBExtensions.java |
| http://jabber.org/protocol/disco#items | asmack/org/jivesoftware/smackx/packet/DiscoverItems.java |
| http://jabber.org/protocol/caps | asmack/org/jivesoftware/smackx/packet/CapsExtension.java |
| http://jabber.org/protocol/caps' | asmack/org/jivesoftware/smackx/packet/CapsExtension.java |
| http://jabber.org/protocol/nick | asmack/org/jivesoftware/smackx/packet/Nick.java |
| http://jabber.org/protocol/commands | asmack/org/jivesoftware/smackx/packet/AdHocCommandData.java |
| http://jabber.org/protocol/bytestreams | asmack/org/jivesoftware/smackx/packet/Bytestream.java |
| http://jabber.org/protocol/pubsub | asmack/org/jivesoftware/smackx/packet/PEPPubSub.java |
| http://www.jivesoftware.org/protocol/sharedgroup | asmack/org/jivesoftware/smackx/packet/SharedGroupsInfo.java |
| http://jabber.org/protocol/chatstates | asmack/org/jivesoftware/smackx/packet/ChatStateExtension.java |
| http://jabber.org/protocol/muc | asmack/org/jivesoftware/smackx/packet/MUCInitialPresence.java |
| http://jabber.org/protocol/muc#user | asmack/org/jivesoftware/smackx/packet/MUCUser.java |
| http://jabber.org/protocol/muc#owner | asmack/org/jivesoftware/smackx/packet/MUCOwner.java |
| http://jabber.org/protocol/offline | asmack/org/jivesoftware/smackx/packet/OfflineMessageRequest.java |
| http://jabber.org/protocol/muc#user | asmack/org/jivesoftware/smackx/muc/Occupant.java |
| http://jivesoftware.org/protocol/muc | asmack/org/jivesoftware/smackx/muc/DeafOccupantInterceptor.java |
| http://jabber.org/protocol/muc | asmack/org/jivesoftware/smackx/muc/DeafOccupantInterceptor.java |
| http://jabber.org/protocol/muc#user | asmack/org/jivesoftware/smackx/muc/PacketMultiplexListener.java |
| http://jabber.org/protocol/muc | asmack/org/jivesoftware/smackx/muc/MultiUserChat.java |
| http://jabber.org/protocol/muc#rooms | asmack/org/jivesoftware/smackx/muc/MultiUserChat.java |
| http://jabber.org/protocol/muc#user | asmack/org/jivesoftware/smackx/muc/MultiUserChat.java |
| http://jabber.org/protocol/commands | asmack/org/jivesoftware/smackx/commands/AdHocCommandManager.java |
| http://jabber.org/protocol/ibb | asmack/org/jivesoftware/smackx/filetransfer/IBBTransferNegotiator.java |
| http://jabber.org/protocol/bytestreams | asmack/org/jivesoftware/smackx/filetransfer/Socks5TransferNegotiator.java |
| http://jabber.org/protocol/bytestreams | asmack/org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java |
| http://jabber.org/protocol/ibb | asmack/org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java |
| http://jabber.org/protocol/si/profile/file-transfer | asmack/org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java |
| http://jabber.org/protocol/si | asmack/org/jivesoftware/smackx/filetransfer/FileTransferNegotiator.java |
| http://jabber.org/protocol/bytestreams | asmack/org/jivesoftware/smackx/filetransfer/Socks5TransferNegotiatorManager.java |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libuptsmaddon.so |
| http://client.map.baidu.com/imap/sdk/tj?qt=vmap | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://v.map.baidu.com/low/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://v.map.baidu.com/indoorinside/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://v.map.baidu.com/high/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://its.map.baidu.com:8003/its.php | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://wp.map.baidu.com/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://api.map.baidu.com/sdkws/heatmap? | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://sv.map.baidu.com/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://sv0.map.bdimg.com/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://client.map.baidu.com/?qt=rg&mmproxyver=1&url= | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://client.map.baidu.com/rchksdk.dat? | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://client.map.baidu.com/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.so |
| http://client.map.baidu.com/phpui2/ | lib/armeabi-v7a/libBaiduMapSDK\_v3\_5\_0\_1.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 |
| http://101.231.114.238:5089/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.204.80:16005/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.224:11000/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| http://172.17.236.169:8081/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.217:8080/app/mobile/conf | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.204.80:16005/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.224:11000/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.217:8080/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://172.17.236.169:8081/app/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://202.101.25.178:8080/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.224:11000/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://101.231.114.217:8080/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://120.204.69.182:8080/gateway/mobile/json | lib/armeabi-v7a/libentryexpro.so |
| http://www.openssl.org/support/faq.html | lib/armeabi/libuptsmaddon.so |
| http://101.231.114.238:5089/app/mobile/json | lib/armeabi/libentryexpro.so |
| http://101.231.204.80:16005/app/mobile/conf | lib/armeabi/libentryexpro.so |
| http://101.231.114.224:11000/app/mobile/conf | lib/armeabi/libentryexpro.so |
| http://172.17.236.169:8081/app/mobile/conf | lib/armeabi/libentryexpro.so |
| http://101.231.114.217:8080/app/mobile/conf | lib/armeabi/libentryexpro.so |
| http://101.231.204.80:16005/app/mobile/json | lib/armeabi/libentryexpro.so |
| http://101.231.114.224:11000/app/mobile/json | lib/armeabi/libentryexpro.so |
| http://101.231.114.217:8080/app/mobile/json | lib/armeabi/libentryexpro.so |
| http://172.17.236.169:8081/app/mobile/json | lib/armeabi/libentryexpro.so |
| http://202.101.25.178:8080/gateway/mobile/json | lib/armeabi/libentryexpro.so |
| http://101.231.114.224:11000/gateway/mobile/json | lib/armeabi/libentryexpro.so |
| http://101.231.114.217:8080/gateway/mobile/json | lib/armeabi/libentryexpro.so |
| http://120.204.69.182:8080/gateway/mobile/json | lib/armeabi/libentryexpro.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| rubin@rubindemacbook-pro.local | com/netease/yunxin/report/sdk/ReportManager.java |
| rubin@rubindemacbook-pro.local | com/netease/yunxin/nos/sdk/NosFacade.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 14299905835 | lib/armeabi-v7a/libbd\_wsp\_v1\_0.so |
| 15330246164 | lib/armeabi-v7a/libbd\_wsp\_v1\_0.so |
| 14299905835 | lib/armeabi/libbd\_wsp\_v1\_0.so |
| 15330246164 | lib/armeabi/libbd\_wsp\_v1\_0.so |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=cn, ST=beijing, L=haidian, O=taogu, OU=taogu, CN=taogu Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2015-03-31 05:50:47+00:00 Valid To: 2070-01-01 05:50:47+00:00 Issuer: C=cn, ST=beijing, L=haidian, O=taogu, OU=taogu, CN=taogu Serial Number: 0x3fbd26ae Hash Algorithm: sha256 md5: 4fe3b5a9aaa5b4304cc665268b9d6b36 sha1: c415115548daddef41a71d7bdabba4e09cefb4ea sha256: 302b31d8b633ba7a2f34371ff57ce104d187eb7e8be7727644806be9494d8555 sha512: 11d03fceca85d0860cb34f60efa05788658483fb2e337916f19aef6284d8ab30be163c3ce896881434ad243bf3b79aa70d7269da1eae30c6d6ffac51da0c1746 PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: 734f14d4f13a21c3f44cee82bac439f3c100c398b91ce75d8db652eba6c9e2d4**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Please\_enter\_a\_username" : "请输入用户名" |
| "Two\_input\_password" : "两次输入的密码不一致，请重新输入!" |
| "bd\_wallet\_forget\_phone\_pwd" : "忘记手机支付密码" |
| "bd\_wallet\_modify\_phone\_pwd" : "修改手机支付密码" |
| "bd\_wallet\_pay\_security\_set\_pay\_pwd\_tip" : "您尚未设置手机支付密码，请设置后开启隐私安全保护" |
| "bd\_wallet\_phone\_pwd" : "手机支付密码" |
| "bd\_wallet\_set\_phone\_pwd" : "设置手机支付密码" |
| "des\_key" : "543141324f33473455354b3645374a38493931" |
| "doctor\_delete\_user" : "删除当前用户" |
| "ebpay\_check\_pwd" : "验证手机支付密码" |
| "ebpay\_input\_mobile\_pwd" : "输入手机支付密码" |
| "ebpay\_modified\_pwd" : "修改手机支付密码" |
| "ebpay\_no\_pwd\_complete\_tip" : "您尚未设置手机支付密码，为了您的账户安全，请重新填写银行卡信息" |
| "ebpay\_nobalance\_pwd" : "使用余额必须先设置手机支付密码" |
| "ebpay\_noscroe\_pwd" : "使用百赚分必须先设置手机支付密码" |
| "ebpay\_pwd\_changed" : "密码不一致请重新输入" |
| "ebpay\_pwd\_check\_tip" : "请输入手机支付密码以验证身份" |
| "ebpay\_pwd\_check\_tip2" : "请输入旧手机支付密码以验证身份" |
| "ebpay\_pwd\_confim\_tip" : "请确认手机支付密码" |
| "ebpay\_pwd\_done" : "完成" |
| "ebpay\_pwd\_forget" : "忘记密码？" |
| "ebpay\_pwd\_forget\_success" : "密码找回成功" |
| "ebpay\_pwd\_set\_tip" : "仅用于手机支付的数字密码，以后凭该密码安全支付，请勿与登录密码设置一致" |
| "ebpay\_pwdpay\_balance\_pay" : "余额支付" |
| "ebpay\_pwdpay\_balance\_pre" : "余额%1$s元(本单可用%2$s元)" |
| "ebpay\_pwdpay\_bankcard" : "银行卡" |
| "ebpay\_pwdpay\_continue" : "继续" |
| "ebpay\_pwdpay\_first\_launch\_tip" : "百赚分/余额/银行卡，更多组合选择 ↗" |
| "ebpay\_pwdpay\_payment\_pre" : "支付方式:%1$s" |
| "ebpay\_pwdpay\_payment\_select" : "选择支付方式" |
| "ebpay\_pwdpay\_score\_pre" : "百赚分%1$s点(本单可用%2$s元,扣减%3$s点)" |
| "ebpay\_set\_pwd\_success" : "新密码设置成功" |
| "ebpay\_tip\_find\_pwd" : "请重新绑定本人银行卡以找回密码" |
| "ebpay\_tobe\_active\_set\_pwd\_tips" : "为了您的账户安全，设置手机支付密码前请绑定本人银行卡以验证身份" |
| "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\_key" : "nrtc\_setting\_vie\_crop\_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\_dtx\_key" : "nrtc\_setting\_voe\_dtx\_key" |
| "nrtc\_setting\_voe\_high\_quality\_key" : "nrtc\_setting\_voe\_high\_quality\_key" |
| "phone\_authentication" : "手机号认证" |
| "private\_allowjoinme" : "允许别人加我为好友" |
| "private\_joinmeneedverify" : "加我为好友时需要验证" |
| "real\_auth\_ID\_card" : "请拍摄/上传您的身份证" |
| "reset\_password" : "忘记密码" |
| "reset\_pwd\_is\_null" : "确认密码不能为空" |
| "session" : "信息" |
| "session\_with\_count" : "信息(%1$s)" |
| "set\_private" : "隐私" |
| "set\_pwd\_is\_null" : "请输入新密码" |
| "two\_pwd\_diff" : "两次输入的密码不一致" |
| "verify\_password" : "确认密码" |
| "wallet\_base\_set\_pwd\_tips" : "你还没有设置六位支付密码，暂时不能使用余额支付，点我开启" |
| "yb\_pwd" : "请输入医保密码" |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.MANAGE\_DOCUMENTS | 合法 |  | 允许应用程序管理对文档的访问,通常作为文档选择器的一部分 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| android.permission.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.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.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 |
| android.permission.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_FINE\_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.USE\_CREDENTIALS | 危险 | 使用帐户的身份验证凭据 | 允许应用程序请求身份验证令牌 |
| android.permission.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| android.permission.AUTHENTICATE\_ACCOUNTS | 危险 | 充当帐户验证器 | 允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| getui.permission.GetuiService.com.hbstss.cfdhsjyfwpt | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.hbstss.cfdhsjyfwpt.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.BLUETOOTH | 正常 | 创建蓝牙连接 | 允许应用程序连接到配对的蓝牙设备 |
| android.permission.BLUETOOTH\_ADMIN | 正常 | 蓝牙管理 | 允许应用程序发现和配对蓝牙设备。 |
| android.permission.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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.toogoo.appbase.webview.SchemeActivity | **Schemes**: taogu://, |
| com.toogoo.appbase.h5link.H5LinkActivity | **Schemes**: com.hbstss.cfdhsjyfwpt://, |

**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。**