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

**天猫国际专用（ 100.11.5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 | 天猫国际专用 |
| 版本 | 100.11.5 |
| 包名 | com.s1780tianmaoguoji.chat |
| 域名线索 | 77条 |
| URL线索 | 53条 |
| APP图标 |  |
| 分析日期 | 2024年11月22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 | deae3ec09dd78a3a318f9eb036afeecd.apk |
| 文件大小 | 33.64MB |
| MD5值 | 3c174f85308622cadb6591d4723b48f5 |
| SHA1值 | ab64bb8e5379eae40c2c212df2e0ab2222f7f292 |
| SHA256值 | 764deeb543dd528469d57f1f87fecc3285ade8da5719af234416b3d210df1dc0 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 天猫国际专用 |
| 包名 | com.s1780tianmaoguoji.chat |
| 主活动Activity | com.gaoyuan.mianshu.main.activity.SplashActivity |
| 安卓版本名称 | 100.11.5 |
| 安卓版本 | 109 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| store2.hispace.hicloud.com | IP: 18.65.168.75 所属国家: United States of America 地区: Washington 城市: Seattle  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Beijing 城市: Beijing  |
| lbs.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| wb.amap.com | IP: 59.82.60.46 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-push.meizu.com | IP: 125.94.213.129 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| nosup-hz1.127.net | IP: 45.127.129.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| webrd0d.is.autonavi.com | 没有服务器地理信息.  |
| cgicol.amap.com | IP: 59.82.31.156 所属国家: China 地区: Beijing 城市: Beijing  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| lbs.chatnos.com | IP: 59.111.211.13 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.jivesoftware.com | IP: 35.238.7.255 所属国家: United States of America 地区: Iowa 城市: Council Bluffs  |
| 169.254.170.2 | IP: 169.254.170.2 所属国家: - 地区: - 城市: -  |
| grs.dbankcloud.asia | 没有服务器地理信息.  |
| check-ipv4.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| xmlpull.org | IP: 74.50.61.58 所属国家: United States of America 地区: Texas 城市: Dallas  |
| wap.amap.com | IP: 182.40.18.221 所属国家: China 地区: Shandong 城市: Qingdao  |
| mst0d.is.autonavi.com | 没有服务器地理信息.  |
| maps.google.cn | IP: 220.181.174.98 所属国家: China 地区: Beijing 城市: Beijing  |
| imtest.netease.im | IP: 59.111.241.163 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| norma-external-collect.meizu.com | IP: 113.106.27.98 所属国家: China 地区: Guangdong 城市: Zhongshan  |
| 169.254.169.254 | IP: 169.254.169.254 所属国家: - 地区: - 城市: -  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| m5.amap.com | IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| trs1780fe.s3.ap-northeast-2.amazonaws.com | IP: 52.219.58.67 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| wannos.127.net | IP: 223.252.196.43 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| lbs.amap.com | IP: 59.82.29.231 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| rs.qiniu.com | IP: 111.225.212.229 所属国家: China 地区: Hebei 城市: Langfang  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| store-drru.hispace.hicloud.com | IP: 159.138.202.186 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| apiinit.amap.com | IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| lbs-test.netease.im | IP: 59.111.211.9 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| nim.nosdn.127.net | IP: 182.40.61.243 所属国家: China 地区: Shandong 城市: Qingdao  |
| 59.111.110.28 | IP: 59.111.110.28 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apilocatesrc.amap.com | IP: 106.11.43.81 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| restapi.amap.com | IP: 203.119.175.194 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| logs.amap.com | IP: 59.82.60.46 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| store.hispace.hicloud.com | IP: 49.4.32.127 所属国家: China 地区: Beijing 城市: Beijing  |
| 45.127.128.25 | IP: 45.127.128.25 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| fr.register.xmpush.global.xiaomi.com | IP: 3.122.79.134 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| metrics-dra.dt.hicloud.com | IP: 94.74.80.173 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| s3.amazonaws.com | IP: 52.217.75.134 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| tm.amap.com | IP: 59.82.31.164 所属国家: China 地区: Beijing 城市: Beijing  |
| store1.hispace.hicloud.com | IP: 49.4.44.164 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.cn | IP: 49.4.41.160 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| api.xmpush.xiaomi.com | IP: 118.26.252.230 所属国家: China 地区: Beijing 城市: Beijing  |
| 154.197.24.8 | IP: 154.197.24.8 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| grid.amap.com | IP: 203.119.145.40 所属国家: China 地区: Beijing 城市: Beijing  |
| idmb.register.xmpush.global.xiaomi.com | IP: 13.235.176.185 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| appgallery.cloud.huawei.com | IP: 121.36.118.136 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 121.36.119.243 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| data-drcn.push.dbankcloud.com | IP: 121.36.117.8 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics1.data.hicloud.com | IP: 114.115.188.66 所属国家: China 地区: Beijing 城市: Beijing  |
| www.w3.org | IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| cn.register.xmpush.xiaomi.com | IP: 118.26.252.220 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| statistic.live.126.net | IP: 183.136.182.46 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| resolver.msg.xiaomi.net | IP: 120.92.96.13 所属国家: China 地区: Beijing 城市: Beijing  |
| store-at-dre.hispace.dbankcloud.com | IP: 80.158.5.6 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| nos.netease.com | IP: 45.127.129.37 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store3.hispace.hicloud.com | IP: 104.94.253.2 所属国家: United States of America 地区: Georgia 城市: Atlanta  |
| app.netease.im | IP: 59.111.243.80 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| trs1780fe.oss-ap-northeast-2.aliyuncs.com | IP: 149.129.12.33 所属国家: Korea (Republic of) 地区: Seoul-teukbyeolsi 城市: Seoul  |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| new.api.ad.xiaomi.com | 没有服务器地理信息.  |
| yunxin.163.com | IP: 59.111.243.80 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| dr.netease.im | IP: 183.131.177.88 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| check-ipv6.netease.im | 没有服务器地理信息.  |
| 45.127.128.24 | IP: 45.127.128.24 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| gitee.com | IP: 182.255.34.126 所属国家: China 地区: Shanghai 城市: Shanghai  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/et.java  |
| http://cgicol.amap.com/collection/writedata?ver=v1.0\_ali&  | com/amap/api/col/hi.java  |
| http://restapi.amap.com/v3/geocode/regeo  | com/amap/api/col/hi.java  |
| http://tm.amap.com  | com/amap/api/col/bg.java  |
| http://wprd0%d.is.autonavi.com  | com/amap/api/col/bg.java  |
| http://webrd0%d.is.autonavi.com  | com/amap/api/col/bg.java  |
| http://grid.amap.com/grid/%d/%d/%d?ds=  | com/amap/api/col/bg.java  |
| http://mst0%d.is.autonavi.com  | com/amap/api/col/bg.java  |
| http://restapi.amap.com/v3  | com/amap/api/col/dc.java  |
| https://restapi.amap.com/v3  | com/amap/api/col/dc.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/dc.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/dc.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/dc.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/dc.java  |
| http://restapi.amap.com/v3/place/around?  | com/amap/api/col/a.java  |
| http://restapi.amap.com/v3/place/text?  | com/amap/api/col/a.java  |
| http://restapi.amap.com/v3/config/district?  | com/amap/api/col/a.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/eo.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/eo.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/eo.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/eo.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/amap/api/col/es.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/col/f.java  |
| http://apilocatesrc.amap.com/mobile/binary  | com/amap/api/col/f.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/amap/api/col/f.java  |
| http://logs.amap.com/ws/log/upload?product=%s&type=%s&platform=%s&channel=%s&sign=%s  | com/amap/api/col/fd.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/amap/api/col/ia.java  |
| http://restapi.amap.com  | com/amap/api/col/ey.java  |
| http://wap.amap.com/  | com/amap/api/maps2d/AMapUtils.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| https://api.xmpush.xiaomi.com/upload/xmsf\_log?file=  | com/xiaomi/mipush/sdk/u.java  |
| https://api.xmpush.xiaomi.com/upload/app\_log?file=  | com/xiaomi/mipush/sdk/u.java  |
| https://api.xmpush.xiaomi.com/upload/crash\_log?file=  | com/xiaomi/mipush/sdk/w.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gt.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/fq.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gs.java  |
| http://new.api.ad.xiaomi.com/logNotificationAdActions  | com/xiaomi/push/cs.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/gl.java  |
| http://%1$s/gslb/?ver=4.0  | com/xiaomi/push/db.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/ga.java  |
| http://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bc.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/l.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/l.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/l.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/l.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/l.java  |
| http://statistic.live.126.net/statics/report/common/form  | com/netease/nimlib/d/g/a.java  |
| https://statistic.live.126.net/dispatcher/req  | com/netease/nimlib/c/b.java  |
| https://statistic.live.126.net/  | com/netease/nimlib/c/b/d/b.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://nosup-hz1.127.net  | com/netease/nimlib/f/g.java  |
| https://lbs-test.netease.im/lbs/conf.jsp  | com/netease/nimlib/f/e.java  |
| https://imtest.netease.im/1.gif  | com/netease/nimlib/f/e.java  |
| http://check-ipv4.netease.im/  | com/netease/nimlib/f/e.java  |
| http://check-ipv6.netease.im/  | 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  |
| 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://api-push.meizu.com  | com/meizu/cloud/pushsdk/b/c/e.java  |
| http://second  | com/gaoyuan/mianshu/f.java  |
| http://second  | com/gaoyuan/mianshu/NimApplication.java  |
| http://59.111.110.28:8281/lbs/demoConfig.jsp  | com/gaoyuan/mianshu/main/activity/PrivatizationConfigActivity.java  |
| http://maps.google.cn/maps/api/staticmap?size=200x100&zoom=13&markers=color:red  | com/gaoyuan/mianshu/location/activity/LocationAmapActivity.java  |
| https://nim.nosdn.127.net/MTAxMTAxMA==/bmltYV8yNDM0MzQ4OV8xNTMyMDUzNzM3ODkzXzJlNGQ3ZjA5LWI2MjgtNDNiNy1hZTIwLTBhYTgzMjZhYzBjZQ==?thumbnail=540x540&imageView&tostatic=0  | com/gaoyuan/mianshu/chatroom/activity/ChatRoomActivity.java  |
| https://app.netease.im/api/  | com/gaoyuan/mianshu/j/a/a.java  |
| http://rs.qiniu.com/stat/aGVhZHBpYy1hOmhlYWRpY29uLnBuZw==  | com/gaoyuan/mianshu/network/MyGitFile$mListqQnNew$2.java  |
| http://rs.qiniu.com/stat/aGVhZHBpYy1iOmhlYWRpY29uLnBuZw==  | com/gaoyuan/mianshu/network/MyGitFile$mListqQnNew$2.java  |
| http://rs.qiniu.com/stat/aGVhZHBpYy1jOmhlYWRpY29uLnBuZw==  | com/gaoyuan/mianshu/network/MyGitFile$mListqQnNew$2.java  |
| https://gitee.com/  | com/gaoyuan/mianshu/network/MyGitFile$testGit$1.java  |
| http://154.197.24.8/  | com/gaoyuan/mianshu/network/MyGitFile.java  |
| http://rs.qiniu.com  | com/gaoyuan/mianshu/network/MyGitFile$testQn$1.java  |
| https://gitee.com/jianliao/project1/raw/master/readme.md  | com/gaoyuan/mianshu/network/MyGitFile$mList$2.java  |
| https://gitee.com/ccdfddxcg/mytest/raw/master/readme.md  | com/gaoyuan/mianshu/network/MyGitFile$mList$2.java  |
| https://gitee.com/zhang-zhenyue/kratos/raw/master/readme.md  | com/gaoyuan/mianshu/network/MyGitFile$mList$2.java  |
| https://gitee.com/ph-on/gateway/raw/master/readme.md  | com/gaoyuan/mianshu/network/MyGitFile$mList$2.java  |
| https://trs1780fe.oss-ap-northeast-2.aliyuncs.com/czE3ODA%3D  | Mogua Engine V1  |
| https://trs1780fe.s3.ap-northeast-2.amazonaws.com/czE3ODA%3D  | 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://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | 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://store1.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| 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://statistic.live.126.net  | lib/x86/libhigh-available.so  |
| https://lbs.netease.im/lbs/conf.jsp  | lib/x86/libhigh-available.so  |
| https://lbs.chatnos.com/lbs/conf.jsp  | lib/x86/libhigh-available.so  |
| https://yunxin.163.com/lbs/conf.jsp  | lib/x86/libhigh-available.so  |
| http://45.127.128.24  | lib/x86/libhigh-available.so  |
| http://45.127.128.25  | lib/x86/libhigh-available.so  |
| http://nos.netease.com  | lib/x86/libhigh-available.so  |
| http://s3.amazonaws.com/doc/2006-03-01/  | lib/x86/libhigh-available.so  |
| http://www.w3.org/2001/XMLSchema-instance  | lib/x86/libhigh-available.so  |
| http://169.254.170.2  | lib/x86/libhigh-available.so  |
| http://169.254.169.254  | lib/x86/libhigh-available.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com  | lib/x86/libhigh-available.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: False v3 signature: False Found 1 unique certificates Subject: C=cn, ST=hunan, L=changsha, O=ec61bb5b03d5e763cece2c, OU=83a8d144e2f404b10c, CN=2812bf1ae16c Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2022-02-27 10:10:06+00:00 Valid To: 2039-05-29 10:10:06+00:00 Issuer: C=cn, ST=hunan, L=changsha, O=ec61bb5b03d5e763cece2c, OU=83a8d144e2f404b10c, CN=2812bf1ae16c Serial Number: 0x23d42ee13e86e91c Hash Algorithm: sha256 md5: 13759cf06f13c6c1de2b852a395b05d2 sha1: 0c4533f6b812c9ecae03bd05622589439b52d85d sha256: c222e63e4c5bbbb95d455dd1c14a10c6937ccb8f1b2bbeef02c37feced9e2253 sha512: 6c97df02d337dc6536b49029175cd08b2b066f694d66108079efd1c20907cefbba31c6a45a009a29a5ef95002734542a0bda044090cd93d3365f3ea9941e9dfd**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "cloud\_session\_list" : "云端会话列表"  |
| "input\_password" : "请输入密码，6~20位字母或者数字"  |
| "main\_tab\_session" : "会话"  |
| "meizuKey" : "11111111111111111111111111111111"  |
| "no\_more\_session" : "没有更多会话了"  |
| "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"  |
| "view\_cloud\_session" : "查看云端会话"  |
| "xiaomiKey" : "11111111111111"  |

## **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.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.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\_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.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\_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.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.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 |
| 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.vivo.notification.permission.BADGE\_ICON | 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。 |
| com.s1780tianmaoguoji.chat.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.s1780tianmaoguoji.chat.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.s1780tianmaoguoji.chat.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 |
| com.s1780tianmaoguoji.chat.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 |
| com.s1780tianmaoguoji.chat.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.s1780tianmaoguoji.chat.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| 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**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.gaoyuan.mianshu.main.activity.SplashActivity | **Schemes**: xxxxxx://,  |
| com.gaoyuan.mianshu.main.activity.MixPushActivity | **Schemes**: pushscheme://, **Hosts:** com.huawei.codelabpush, **Paths:** /deeplink,  |

**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。**