MoGua

移动平台 2.2.0.APK 分析报告

APP名称: 移动平台

包名:	cn.com.petrochina.EnterpriseHall
域名线索:	38条
URL线索:	49条
邮箱线索:	13条
分析日期:	2025年5月5日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app-release (1).apk
文件大小: 61.75MB
MD5值: b928f7f56f1433ad4f7c3d4efb0ce932
SHA1值: 6f43951e6c486dda8ccb41533e2a301d00e9cb35
SHA256值: e8d3a7a374b22d31fcb21e47279f0f808d88f1383f616e1f96d6d6607881122e

APP 信息

App名称: 移动平台
包名: cn.com.petrochina.EnterpriseHall
主活动Activity: cn.com.petrochina.EnterpriseHall.action.Welcome
安卓版本名称: 2.2.0
安卓版本: 27

域名线索

域名	服务器信息
mdm.cnpc.com.cn	**IP**: 106.38.74.217 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
v4.ident.me	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
	IP: 116.130.223.156 **所属国家**: China **地区**: Beijing

ue.indoorloc.map.qq.com	**城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
msso.iam.cnpc.com.cn	IP: 111.203.165.45 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
zxcv.3g.qq.com	IP: 0.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
wup.imtt.qq.com	IP: 125.39.104.63 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
pv.sohu.com	IP: 101.72.254.86 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
github.com	IP: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

111.203.165.45	**IP**: 111.203.165.45 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ip.42.pl	没有服务器地理信息.
ip-api.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
mdc.html5.qq.com	**IP**: 116.130.223.178 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cfg.imtt.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
xmlpull.org	**IP**: 185.199.110.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
	IP: 111.206.174.248 **所属国家**: China

resolver.msg.xiaomi.net	**地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.trackip.net	IP: 172.67.153.101 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
bj.npc5sgft.76d90eb7.com	没有服务器地理信息.
106.39.36.194	IP: 106.39.36.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
lbs.map.qq.com	IP: 116.130.220.64 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.jivesoftware.com	IP: 23.235.209.143 **所属国家**: United States of America **地区**: Virginia **城市**: Virginia Beach **纬度**: 36.837925 **经度**: -76.093918
debugtbs.qq.com	IP: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181

	经度: 117.176102
open.hicloud.com	没有服务器地理信息.
javascript.crockford.com	**IP**: 217.160.0.111 **所属国家**: Germany **地区**: Nordrhein-Westfalen **城市**: Strang **纬度**: 51.968700 **经度**: 8.753360
lstest.map.qq.com	**IP**: 116.130.223.83 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
demo.com	**IP**: 151.101.2.165 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
pms.mb.qq.com	**IP**: 60.29.240.17 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

myip.fireflysoft.net	IP: 123.57.80.7 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
data.hicloud.com	IP: 118.194.33.124 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
debugx5.qq.com	IP: 60.29.240.122 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
abc.test.com	IP: 69.167.164.199 **所属国家**: United States of America **地区**: Michigan **城市**: Lansing **纬度**: 42.733280 **经度**: -84.637764
bj.npc5sgft.27870d11.com	没有服务器地理信息.
emp.cnpc.com.cn	IP: 114.255.212.39 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 0.0.0.1 **所属国家**: -

mqqad.html5.qq.com	**地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
log.tbs.qq.com	**IP**: 124.95.224.248 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
www.json.org	**IP**: 74.208.236.169 **所属国家**: United States of America **地区**: Pennsylvania **城市**: Philadelphia **纬度**: 39.962440 **经度**: -75.199928
ip.qiyutech.tech	**IP**: 121.196.187.108 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
soft.tbs.imtt.qq.com	**IP**: 119.167.147.86 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941

URL线索

URL信息	Url所在文件

http://bj.npc5sgft.76d90eb7.com/PT_ZEMMV2Api/api/	cn/com/petrochina/rcgl/a/c.java
https://106.39.36.194:10443	cn/com/petrochina/ydpt/home/MPApplication.java
https://mdm.cnpc.com.cn/PT_ZEMMV2ApiExt/api/app/GetAuthAppBundleIdList?user_token=	cn/com/petrochina/ydpt/home/help/ApiManagerHelper.java
https://106.39.36.194:10443	cn/com/petrochina/ydpt/home/help/a.java
https://mdm.cnpc.com.cn/PT_SendSMS/api/Verify/SendSMSDevVerifyCode	cn/com/petrochina/ydpt/home/network/c.java
https://mdm.cnpc.com.cn/PT_ZEMMV2ApiExt/api/	cn/com/petrochina/ydpt/home/network/e.java
http://bj.npc5sgft.76d90eb7.com/PT_ZEMMV2Api/api/	cn/com/petrochina/ydpt/home/network/e.java
http://demo.com/	cn/com/petrochina/ydpt/home/network/e.java
http://bj.npc5sgft.76d90eb7.com/PT_ZEMMV2Api/api/	cn/com/petrochina/ydpt/home/cordova/plugins/GetUrlParamsPlugin.java
https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/WebAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/login/updatePwd	cn/com/petrochina/ydpt/home/action/ModifyIAMPswdAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/login/sms	cn/com/petrochina/ydpt/home/action/VerifyIAMPhoneAction.java
https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/RegisterMobilePhoneAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/loginByPhone	cn/com/petrochina/ydpt/home/action/IdentifyBindingAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/verifyCode/sendByPhone	cn/com/petrochina/ydpt/home/action/IdentifyBindingAction.java
https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/NewDeviceLoginAction.java
http://bj.npc5sgft.76d90eb7.com/PT_ZEMMV2Api//api/App/GetAppList	cn/com/petrochina/ydpt/home/action/NewDeviceLoginAction.java
https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/CordovaAppNewAction.java

https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/IAMUserLoginAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/loginByPhone	cn/com/petrochina/ydpt/home/action/IAMUserLoginAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/verifyCode/sendByPhone	cn/com/petrochina/ydpt/home/action/IAMUserLoginAction.java
https://emp.cnpc.com.cn/)	cn/com/petrochina/ydpt/home/action/SplashAction.java
https://emp.cnpc.com.cn/	cn/com/petrochina/ydpt/home/action/SplashAction.java
https://emp.cnpc.com.cn/ZEMMPortal/AppHelp	cn/com/petrochina/ydpt/home/action/UserLoginAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/loginByPhone	cn/com/petrochina/ydpt/home/action/UserLoginAction.java
https://111.203.165.45:5889/ngiam-rst/v1/sdk/client/verifyCode/sendByPhone	cn/com/petrochina/ydpt/home/action/UserLoginAction.java
http://bj.npc5sgft.27870d11.com/BHZTMobile/api/Module/SiteList?LoginId=15571969903	cn/com/petrochina/ydpt/home/action/SecureVerifyAction.java
https://106.39.36.194:10443	cn/com/petrochina/ydpt/home/action/HomeReactAction.java
http://open.hicloud.com/android/push1.0.js	com/huawei/android/pushselfshow/richpush/html/HtmlViewer.java
http://open.hicloud.com/android/push1.0.js\	com/huawei/android/pushselfshow/richpush/html/e.java
https://msso.iam.cnpc.com.cn:5889/ngiam-rst	com/jingan/sdk/CoreLibConfig.java
http://karsten:password@abc.test.com:8080	com/jnsec/jce/provider/test/PKIXNameConstraintsTest.java
http://data.hicloud.com:8089/sdkv1	com/hianalytics/android/a/a/a.java
http://ip-api.com/json/?lang=zh-CN	com/msmsdk/f/j.java
https://pv.sohu.com/cityjson	com/msmsdk/f/d.java

https://pv.sohu.com/cityjson?ie=utf-8	com/msmsdk/f/d.java
https://www.trackip.net/ip	com/msmsdk/f/d.java
https://v4.ident.me/	com/msmsdk/f/d.java
https://myip.fireflysoft.net/	com/msmsdk/f/d.java
http://ip-api.com/json/?lang=zh-CN	com/msp/a/l.java
https://www.trackip.net/ip	com/msp/a/l.java
https://v4.ident.me/	com/msp/a/l.java
https://myip.fireflysoft.net/	com/msp/a/l.java
https://ip.qiyutech.tech/	com/msp/a/l.java
http://ip.42.pl/raw	com/msp/a/l.java
http://xml.apache.org/xslt	com/orhanobut/logger/LoggerPrinter.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://%1$s/gslb/gslb/getbucket.asp?ver=3.0	com/xiaomi/network/f.java
http://%1$s/gslb/?ver=3.0	com/xiaomi/network/g.java
http://resolver.msg.xiaomi.net/psc/?t=a	com/xiaomi/push/service/u.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/smack/g.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/smack/c/c.java
http://www.jivesoftware.com/xmlns/xmpp/properties\	com/xiaomi/smack/packet/d.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/smack/d/a.java
http://xmlpull.org/v1/doc/features.html	com/xiaomi/c/e.java

http://lbs.map.qq.com/loc?c=1&mars=	ct/bu.java
http://ue.indoorloc.map.qq.com	ct/bg.java
http://zxcv.3g.qq.com/sdk/beacon.jsp?type=real&size=	ct/ar.java
http://lstest.map.qq.com/stat	ct/cx.java
https://github.com/vinc3m1	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView	摸瓜V1引擎
https://github.com/vinc3m1/RoundedImageView.git	摸瓜V1引擎
http://www.JSON.org/json2.js	摸瓜V2引擎
http://www.JSON.org/js.html	摸瓜V2引擎
http://javascript.crockford.com/jsmin.html	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
calendarmanager@gmail.com	cn/com/petrochina/rcgl/b/f.java
xxxx@xxxx.com	com/huawei/android/pushselfshow/utils/a.java
password@abc.test test@abc.test test1@abc.test test@test.com test@test.abc	com/jnsec/jce/provider/test/PKIXNameConstraintsTest.java

feedback-crypto@bouncycastle.org	com/jnsec/jce/provider/test/CertUniqueIDTest.java
feedback-crypto@bouncycastle.org	com/jnsec/jce/provider/test/KeyStoreTest.java
dau123456789@test.com	com/jnsec/jce/provider/test/AttrCertSelectorTest.java
mlorch@vt.edu	com/jnsec/jce/provider/test/AttrCertTest.java
feedback-crypto@bouncycastle.org	com/jnsec/jce/provider/test/PKCS10CertRequestTest.java
issuer@bouncycastle.org subject@bouncycastle.org extra@bouncycaste.org	com/jnsec/jce/provider/test/PKCS12StoreTest.java
feedback-crypto@bouncycastle.org test@test.test	com/jnsec/jce/provider/test/CertTest.java
feedback-crypto@bouncycastle.org	com/jnsec/jce/examples/PKCS12Example.java
eric@bouncycastle.org	com/jnsec/ocsp/test/OCSPTest.java
feedback-crypto@bouncycastle.org	com/jnsec/x509/examples/AttrCertExample.java

手机线索

手机号	所在文件
15571969903	cn/com/petrochina/ydpt/home/action/SecureVerifyAction.java
13516237631	com/haibin/calendarview/SolarTermUtil.java
17882652114	com/haibin/calendarview/SolarTermUtil.java

18914945834	com/haibin/calendarview/SolarTermUtil.java
16832995016	com/haibin/calendarview/SolarTermUtil.java
13846158196	com/haibin/calendarview/SolarTermUtil.java
17471680261	com/haibin/calendarview/SolarTermUtil.java
18826691036	com/haibin/calendarview/SolarTermUtil.java
14159265359	com/haibin/calendarview/SolarTermUtil.java
13446589358	com/haibin/calendarview/SolarTermUtil.java
19870156017	com/haibin/calendarview/SolarTermUtil.java
19846674381	com/haibin/calendarview/SolarTermUtil.java
17387749012	com/haibin/calendarview/SolarTermUtil.java
15095675534	com/jnsec/asn1/ua/DSTU4145NamedCurves.java
14040302010	com/jnsec/jce/provider/test/PKIXTest.java
17751197731	com/jnsec/jce/provider/test/PKIXPolicyMappingTest.java
17751197731	com/jnsec/jce/examples/PKCS12Example.java
17179869184	com/jnsec/pqc/math/linearalgebra/GF2nONBElement.java
17179869183	com/jnsec/pqc/math/linearalgebra/GF2nONBElement.java
17434386626	com/jnsec/security/ec/NamedCurve.java

17751197731	com/jnsec/x509/examples/AttrCertExample.java

签名证书

APK已签名
v1 签名: True
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=SH, ST=河北省, L=廊坊, O=中国石油-万岩通, OU=petrochina, CN=Pan Xiaohua
签名算法: rsassa_pkcs1v15
有效期自: 2013-05-20 09:36:28+00:00
有效期至: 2068-02-21 09:36:28+00:00
发行人: C=SH, ST=河北省, L=廊坊, O=中国石油-万岩通, OU=petrochina, CN=Pan Xiaohua
序列号: 0x5199ee9c
哈希算法: sha1
md5值: e8339f9047e5e2d18de09fbb5e6e8e3f
sha1值: 8b0b1e1e3c4f92fd8d767834db013e6fe8c63ef3
sha256值: 43676de36884c99643091ad331f64a68c9a5dd15026b7e32a389071fa9188870
sha512值: 2478887594a7b14401e2b4def1ba9c4e41b234d91a21f1d9817633fd611734a076ed71cf25055ddcda538d616d1ecc029d5f2be20fcd4d7b5799de1cc77b8381
公钥算法: rsa
密钥长度: 1024
指纹: 59e734c14caa9b6273464892c3accbb21838571c83e241f9ea656696d1805004

硬编码敏感信息

可能的敏感信息
"access_secret_key_alert" : "请插入加密机"
"attend_user" : "参 加 人： "
"click_to_authorize" : "Authorize"

"device_register_binding_user" : "该设备正在申请绑定用户，请联系管理员处理"

"get_valid_sec_key" : "验证加密机使用状态..."

"has_no_email_login_user" : "您还未登录邮箱系统，请先登录!"

"is_register_binding_user" : "用户注册审核中 请等待审核通过"

"is_register_no_bind_user" : "设备已注册，但未绑定用户 请您注册用户"

"library_roundedimageview_author" : "Vince Mi"

"library_roundedimageview_authorWebsite" : "https://github.com/vinc3m1"

"menu_user" : "用户信息"

"mobile_phone_is_bind_user" : "该手机号已绑定用户，请重新输入"

"reqeust_no_authorize" : "请求未授权"

"reset_password" : "重置口令"

"secret_key" : "加密机"

"secret_key_is_accessed" : "加密机已插入"

"select_external_user" : "添加外部人员"

"start_getImToken" : "正在获取IM数据..."

"token_invalid" : "Token无效"

"token_is_refreshed" : "Token已成功刷新，请重新请求数据"

"click_to_authorize" : "授权交易"

"click_to_authorize" : "授權交易"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

向手机申请的权限	是否危险	类型	详细情况
android.permission.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
	系统	删除所有应用程序缓	允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访

android.permission.CLEAR_APP_CACHE	需要	存数据	问通常非常受限于系统进程。
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
android.permission.DELETE_PACKAGES	系统需要	删除应用程序	允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序
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。
android.permission.REQUEST_DELETE_PACKAGES	正常		允许应用程序请求删除包
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.USE_FINGERPRINT	正常	allow use of指纹	该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE_BIOMETRIC
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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.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.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.CAMERA	危	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

	险		
org.fidoalliance.uaf.permissions.FIDO_CLIENT	未知	Unknown permission	Unknown permission from android reference
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_CALENDAR	危险	读取日历事件	允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人
android.permission.WRITE_CALENDAR	危险	添加或修改日历事件并向客人发送电子邮件	允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件
cn.com.petrochina.EnterpriseHall.permission.RECEIVE_MSG	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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。

cn.com.petrochina.EnterpriseHall.permission.MIPUSH_RECEIVE	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.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
android.permission.BLUETOOTH_CONNECT	未知	Unknown permission	Unknown permission from android reference
android.permission.BODY_SENSORS	危险		允许应用程序访问来自传感器的数据,用户使用这些数据来测量他/她体内发生的事情,例如心率
android.permission.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息

android.permission.WRITE_SMS	危险	编辑短信或彩信	允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息
android.permission.WRITE_CONTACTS	危险	写入联系人数据	允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据
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.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
cn.com.petrochina.EnterpriseHall.action.Welcome	Schemes: pushscheme://, Hosts: cn.com.petrochina, Paths: /enterprisehall,

---