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

**湾沚防汛巡查（ 1.0.9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 | 湾沚防汛巡查 |
| 版本 | 1.0.9 |
| 包名 | com.jinhe.newwanzhang |
| 域名线索 | 58条 |
| URL线索 | 71条 |
| APP图标 |  |
| 分析日期 | 2025年6月27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 | app.apk |
| 文件大小 | 104.2MB |
| MD5值 | 87832d5c274813cde9257481fab6e467 |
| SHA1值 | 79f581e07736388fbd8bb3413b7925157972751a |
| SHA256值 | 85bc0c3ea5d156de0b77524069291345168fbbd1ece4e0280b56ef4f85336541 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 湾沚防汛巡查 |
| 包名 | com.jinhe.newwanzhang |
| 主活动Activity | com.jinhe.newwanzhang.activity.SplashActivity |
| 安卓版本名称 | 1.0.9 |
| 安卓版本 | 9 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| abroad.apilocate.amap.com | IP: 59.82.44.11 所属国家: China 地区: Shanghai 城市: Shanghai  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| wz.njningtu.com | IP: 223.240.82.123 所属国家: China 地区: Anhui 城市: Hefei  |
| adiu.amap.com | IP: 110.253.189.146 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| api.mapbox.com | IP: 13.35.37.129 所属国家: Taiwan (Province of China) 地区: Taipei 城市: Taipei  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.zhihu.com | IP: 116.196.155.61 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| 211.141.223.166 | IP: 211.141.223.166 所属国家: China 地区: Anhui 城市: Ma'anshan  |
| wzq.wzswj.top | 没有服务器地理信息.  |
| apps.mapbox.com | IP: 3.166.205.110 所属国家: United States of America 地区: Washington 城市: Seattle  |
| dualstack-a.apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.jianshu.com | IP: 39.98.74.233 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api.tianditu.gov.cn | IP: 218.12.76.154 所属国家: China 地区: Hebei 城市: Tangshan  |
| www.mapbox.com | IP: 151.101.40.143 所属国家: United States of America 地区: California 城市: San Francisco  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| restsdk.amap.com | IP: 106.11.43.113 所属国家: China 地区: Beijing 城市: Beijing  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| lbs.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Beijing 城市: Beijing  |
| cw.gzyunjuchuang.com | IP: 38.14.95.188 所属国家: United States of America 地区: District of Columbia 城市: Washington  |
| segmentfault.com | IP: 8.152.202.66 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| juejin.im | IP: 103.136.220.205 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.baidu.com | IP: 110.242.70.57 所属国家: China 地区: Hebei 城市: Baoding  |
| photocdn.sohu.com | IP: 61.49.23.101 所属国家: China 地区: Beijing 城市: Beijing  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| p6-juejin.byteimg.com | IP: 116.136.185.7 所属国家: China 地区: Nei Mongol 城市: Hohhot  |
| wup.imtt.qq.com | IP: 125.39.104.63 所属国家: China 地区: Tianjin 城市: Tianjin  |
| apiinit.amap.com | IP: 59.82.132.217 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| schemas.android.com | 没有服务器地理信息.  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| qm.qq.com | IP: 116.130.223.44 所属国家: China 地区: Beijing 城市: Beijing  |
| t0.tianditu.gov.cn | IP: 49.4.56.26 所属国家: China 地区: Beijing 城市: Beijing  |
| 223.240.82.123 | IP: 223.240.82.123 所属国家: China 地区: Anhui 城市: Hefei  |
| t.1yb.co | IP: 111.230.191.217 所属国家: China 地区: Beijing 城市: Beijing  |
| xml.org | IP: 104.239.142.8 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| wap.amap.com | IP: 116.142.235.227 所属国家: China 地区: Beijing 城市: Beijing  |
| mpsapi.amap.com | IP: 106.11.43.68 所属国家: China 地区: Beijing 城市: Beijing  |
| mp.weixin.qq.com | IP: 220.196.132.78 所属国家: China 地区: Jiangsu 城市: Zhenjiang  |
| cgicol.amap.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| gitee.com | IP: 180.76.199.13 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| user-gold-cdn.xitu.io | 没有服务器地理信息.  |
| mst01.is.autonavi.com | IP: 110.253.189.211 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| www.toutiao.com | IP: 124.95.172.18 所属国家: China 地区: Liaoning 城市: Shenyang  |
| apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wthrcdn.etouch.cn | 没有服务器地理信息.  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| space.bilibili.com | IP: 221.204.56.95 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| www.unkownwebsiteblog.me | IP: 103.224.182.215 所属国家: Australia 地区: Victoria 城市: Beaumaris  |
| dualstack.apilocate.amap.com | IP: 59.82.31.183 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wb.amap.com | IP: 110.253.189.212 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| dualstack-arestapi.amap.com | IP: 59.82.132.217 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://apache.org/xml/features/disallow-doctype-decl  | cn/hutool/core/util/XmlUtil.java  |
| http://xml.org/sax/features/external-general-entities  | cn/hutool/core/util/XmlUtil.java  |
| http://xml.org/sax/features/external-parameter-entities  | cn/hutool/core/util/XmlUtil.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | cn/hutool/core/util/XmlUtil.java  |
| http://xml.apache.org/xslt  | cn/hutool/core/util/XmlUtil.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/col/p0003nstrl/so.java  |
| http://dualstack.apilocate.amap.com/mobile/binary  | com/amap/api/col/p0003nstrl/so.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/col/p0003nstrl/ou.java  |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&  | com/amap/api/col/p0003nstrl/qp.java  |
| http://restsdk.amap.com/v3  | com/amap/api/col/p0003nstrl/is.java  |
| https://restsdk.amap.com/v3  | com/amap/api/col/p0003nstrl/is.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003nstrl/is.java  |
| https://restsdk.amap.com/v4  | com/amap/api/col/p0003nstrl/is.java  |
| http://yuntuapi.amap.com  | com/amap/api/col/p0003nstrl/is.java  |
| https://yuntuapi.amap.com  | com/amap/api/col/p0003nstrl/is.java  |
| http://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003nstrl/is.java  |
| https://restsdk.amap.com/rest/me/cpoint  | com/amap/api/col/p0003nstrl/is.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003nstrl/is.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/col/p0003nstrl/is.java  |
| https://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003nstrl/ny.java  |
| http://restsdk.amap.com/sdk/compliance/params  | com/amap/api/col/p0003nstrl/ny.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003nstrl/my.java  |
| http://restsdk.amap.com/v3/assistant/inputtips?  | com/amap/api/col/p0003nstrl/fm.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/col/p0003nstrl/mp.java  |
| http://restsdk.amap.com/v3/place/text?  | com/amap/api/col/p0003nstrl/a.java  |
| http://restsdk.amap.com/v3/config/district?  | com/amap/api/col/p0003nstrl/a.java  |
| http://restsdk.amap.com/v3/place/around?  | com/amap/api/col/p0003nstrl/a.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/col/p0003nstrl/mo.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/col/p0003nstrl/mo.java  |
| http://restsdk.amap.com/v3/batch?key=  | com/amap/api/col/p0003nstrl/fn.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/col/p0003nstrl/kw.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003nstrl/dc.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/col/p0003nstrl/db.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/col/p0003nstrl/db.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003nstrl/r.java  |
| http://restsdk.amap.com  | com/amap/api/col/p0003nstrl/hd.java  |
| http://restsdk.amap.com/v4  | com/amap/api/col/p0003nstrl/co.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/p0003nstrl/kq.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003nstrl/kq.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/col/p0003nstrl/kq.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/col/p0003nstrl/kq.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\  | com/amap/api/col/p0003nstrl/k.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| http://restsdk.amap.com/v4/stats/alitts  | com/amap/api/navi/core/network/h.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/amap/api/location/AMapLocation.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/  | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java  |
| http://restsdk.amap.com/rest/lbs/dem/dataservice?z=%d&x=%d&y=%d&type=2  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mst01.is.autonavi.com/appmaptile?z=%d&x=%d&y=%d&lang=zh\_cn&size=1&scale=1&style=6  | com/autonavi/base/ae/gmap/TerrainOverlayProvider.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/b.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/utils/g.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/autonavi/aps/amapapi/trans/a.java  |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://restsdk.amap.com/v3/geocode/regeo  | com/autonavi/aps/amapapi/trans/c.java  |
| http://photocdn.sohu.com/tvmobilemvms/20150907/144160323071011277.jpg  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| http://photocdn.sohu.com/tvmobilemvms/20150907/144158380433341332.jpg  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| http://photocdn.sohu.com/tvmobilemvms/20150907/144160286644953923.jpg  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| http://photocdn.sohu.com/tvmobilemvms/20150902/144115156939164801.jpg  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| http://photocdn.sohu.com/tvmobilemvms/20150907/144159406950245847.jpg  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| http://mp.weixin.qq.com/mp/homepage?\_\_biz=Mzg2NjA3NDIyMA==&hid=5&sn=bdee5aafe9cc2e0a618d055117c84139&scene=18  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://p6-juejin.byteimg.com/tos-cn-i-k3u1fbpfcp/463930705a844f638433d1b26273a7cf  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://juejin.im/post/5c3ed1dae51d4543805ea48d  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://user-gold-cdn.xitu.io/2019/1/16/1685563ae5456408?imageView2/0/w/1280/h/960/format/webp/ignore-error/1  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://juejin.im/post/5b480b79e51d45190905ef44  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://user-gold-cdn.xitu.io/2018/7/13/16492d9b7877dc21?imageView2/0/w/1280/h/960/format/webp/ignore-error/1  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://juejin.im/post/5b6b9b49e51d4576b828978d  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://user-gold-cdn.xitu.io/2018/8/9/1651c568a7e30e02?imageView2/0/w/1280/h/960/format/webp/ignore-error/1  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://juejin.im/post/5c6fc0cdf265da2dda694f05  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://user-gold-cdn.xitu.io/2019/2/22/16914891cd8a950a?imageView2/0/w/1280/h/960/format/webp/ignore-error/1  | com/jinhe/newwanzhang/utils/DemoDataProvider.java  |
| https://gitee.com/xuexiangjys/TemplateAppProject/raw/master/LICENSE  | com/jinhe/newwanzhang/utils/Utils.java  |
| https://gitee.com/  | com/jinhe/newwanzhang/utils/sdkinit/XBasicLibInit.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/modules/river/QuestionUploadFragment.java  |
| http://223.240.82.123:6080/arcgis/rest/services/WZHZZ/MapServer/40/query?where=riverid%3D%27  | com/jinhe/newwanzhang/modules/river/InspectionRiverFragment.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/modules/web/CustomWebViewFragment.java  |
| http://223.240.82.123:6080/arcgis/rest/services/WZHZZ/MapServer/40/query?where=riverid%3D%27  | com/jinhe/newwanzhang/modules/Area/InspectionAreaFragment.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/modules/Area/AreaQuestionUploadFragment.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/modules/dike/DikeMainFragment.java  |
| https://wz.njningtu.com:8086/api/  | com/jinhe/newwanzhang/config/Api.java  |
| https://wzq.wzswj.top:8085  | com/jinhe/newwanzhang/config/Api.java  |
| http://223.240.82.123:9015  | com/jinhe/newwanzhang/config/Api.java  |
| https://wz.njningtu.com:8086/newArcgis  | com/jinhe/newwanzhang/config/Api.java  |
| http://223.240.82.123:6080/arcgis/rest/services/WZHZZ/MapServer/41/query?returnGeometry=true&where=1=1&outSR=4326&outFields=\*&inSr=4326&geometry=undefined&geometryType=esriGeometryEnvelope&spatialRel=esriSpatialRelIntersects&geometryPrecision=6&f=json&callback=jsonCallBack471024  | com/jinhe/newwanzhang/config/Api.java  |
| https://www.baidu.com/  | com/jinhe/newwanzhang/core/webview/BaseAgentWebFragment.java  |
| http://www.unkownwebsiteblog.me  | com/jinhe/newwanzhang/core/webview/AgentWebFragment.java  |
| http://cw.gzyunjuchuang.com/  | com/jinhe/newwanzhang/core/webview/AgentWebFragment.java  |
| https://www.baidu.com/  | com/jinhe/newwanzhang/core/webview/XPageWebViewFragment.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/fragment/utilFragment/SeniorBaseFragment.java  |
| http://wthrcdn.etouch.cn/weather\_mini?city=  | com/jinhe/newwanzhang/fragment/utilFragment/SeniorBaseFragment.java  |
| http://api.tianditu.gov.cn/geocoder?postStr=  | com/jinhe/newwanzhang/fragment/main/MainFragment.java  |
| http://211.141.223.166:6080/arcgis/rest/services/jswz/MapServer/export?dpi=96&transparent=true&format=png8&layers=&bbox=  | com/jinhe/newwanzhang/mapbox/layer/LayerElementConfig.java  |
| http://t0.tianditu.gov.cn/DataServer?tk=ac3c69d0b0f1b7aafc7d946ef387ae61&T=cia\_w&x=  | com/jinhe/newwanzhang/mapbox/layer/layerConfig.java  |
| http://t0.tianditu.gov.cn/DataServer?tk=ac3c69d0b0f1b7aafc7d946ef387ae61&T=cva\_w&x=  | com/jinhe/newwanzhang/mapbox/layer/layerConfig.java  |
| http://t0.tianditu.gov.cn/DataServer?tk=ac3c69d0b0f1b7aafc7d946ef387ae61&T=img\_w&X=  | com/jinhe/newwanzhang/mapbox/layer/layerConfig.java  |
| http://t0.tianditu.gov.cn/DataServer?tk=ac3c69d0b0f1b7aafc7d946ef387ae61&T=vec\_w&X=  | com/jinhe/newwanzhang/mapbox/layer/layerConfig.java  |
| http://211.141.223.166:6080/arcgis/rest/services/jswz/MapServer/export?dpi=96&transparent=true&format=png8&layers=&bbox=  | com/jinhe/newwanzhang/mapbox/layer/layerConfig.java  |
| https://api.mapbox.com  | com/mapbox/core/constants/Constants.java  |
| https://www.mapbox.com/help/create-api-access-token/  | com/mapbox/mapboxsdk/Mapbox.java  |
| https://www.mapbox.com/help/first-steps-android-sdk/  | com/mapbox/mapboxsdk/Mapbox.java  |
| https://www.mapbox.com/help/create-api-access-token/  | com/mapbox/mapboxsdk/exceptions/MapboxConfigurationException.java  |
| https://www.mapbox.com/help/first-steps-android-sdk/  | com/mapbox/mapboxsdk/exceptions/MapboxConfigurationException.java  |
| https://apps.mapbox.com/feedback  | com/mapbox/mapboxsdk/maps/AttributionDialogManager.java  |
| https://www.mapbox.com/map-feedback  | com/mapbox/mapboxsdk/maps/AttributionDialogManager.java  |
| https://www.mapbox.com/about/maps/  | com/mapbox/mapboxsdk/attribution/Attribution.java  |
| https://www.mapbox.com/telemetry/  | com/mapbox/mapboxsdk/attribution/Attribution.java  |
| https://www.mapbox.com/feedback/  | com/mapbox/mapboxsdk/attribution/Attribution.java  |
| https://www.mapbox.com/map-feedback/  | com/mapbox/mapboxsdk/attribution/Attribution.java  |
| https://apps.mapbox.com/feedback/  | com/mapbox/mapboxsdk/attribution/Attribution.java  |
| https://www.mapbox.com/telemetry/  | com/mapbox/mapboxsdk/attribution/AttributionParser.java  |
| https://www.mapbox.com/about/maps/  | com/mapbox/mapboxsdk/attribution/AttributionParser.java  |
| http://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/ak.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://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/a/d.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/b/a/d.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/b/a/d.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/v.java  |
| http://wup.imtt.qq.com:8080  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/v.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/v.java  |
| http://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/v.java  |
| http://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/v.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/i.java  |
| http://schemas.android.com/apk/res/android  | com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/Flowable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://www.mapbox.com/telemetry/  | 摸瓜V1引擎  |
| http://qm.qq.com/cgi-bin/qm/qr?k=tiP-E6rDf0y77PRNfp2lNVcc9RsglPCM  | 摸瓜V1引擎  |
| https://gitee.com/xuexiangjys/xuexiangjys  | 摸瓜V1引擎  |
| https://gitee.com/xuexiangjys/Resource/blob/master/doc/sponsor.md  | 摸瓜V1引擎  |
| https://github.com/xuexiangjys/TemplateAppProject  | 摸瓜V1引擎  |
| https://t.1yb.co/71xZ\  | 摸瓜V2引擎  |
| https://github.com/xuexiangjys\  | 摸瓜V2引擎  |
| https://www.zhihu.com/people/xuexiangjys/posts\  | 摸瓜V2引擎  |
| https://juejin.im/user/598feef55188257d592e56ed/posts\  | 摸瓜V2引擎  |
| https://www.jianshu.com/u/6bf605575337\  | 摸瓜V2引擎  |
| https://segmentfault.com/blog/openAndroidX\  | 摸瓜V2引擎  |
| https://space.bilibili.com/483850585/video\  | 摸瓜V2引擎  |
| https://www.toutiao.com/c/user/token/MS4wLjABAAAAqD0Pe01AhT2Hgi3w7HzboVuq57gntoAJJURwAkM3Elv0-EA9WSKUSy1DujIYLAEm/\  | 摸瓜V2引擎  |
| https://gitee.com/xuexiangjys/Resource/blob/master/doc/sponsor.md\  | 摸瓜V2引擎  |
| https://qm.qq.com/cgi-bin/qm/qr?k=i1rhgvRxlJRlJzigL0QemICtkk0H6g3J\  | 摸瓜V2引擎  |
| https://qm.qq.com/cgi-bin/qm/qr?k=\_0IhSCvLxdsgxAIBtTXr\_\_bwsxZl4Eva\  | 摸瓜V2引擎  |
| https://qm.qq.com/cgi-bin/qm/qr?k=GRVNTA4ehFuIUhQwqiZkjqYeQoxRBqCI\  | 摸瓜V2引擎  |
| https://qm.qq.com/cgi-bin/qm/qr?k=0OHp7jgMiF9SsfrzmOaxcauxMP9fZjc3\  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| auth-agent@openssh.com  | cn/hutool/extra/ssh/ChannelType.java  |
| support@mapbox.com  | com/mapbox/services/android/navigation/v5/navigation/TarResponseErrorMap.java  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 16222222222  | com/amap/api/col/p0003nstrl/mo.java  |

## **5. 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=CN, ST=Jiangsu, L=Nanjing, O=TemplateApp, OU=TemplateApp, CN=TemplateAppProject 签名算法: rsassa\_pkcs1v15 有效期自: 2019-07-29 14:27:49+00:00 有效期至: 2044-07-22 14:27:49+00:00 发行人: C=CN, ST=Jiangsu, L=Nanjing, O=TemplateApp, OU=TemplateApp, CN=TemplateAppProject 序列号: 0x16a3aa5c 哈希算法: sha256 md5值: 97670f380d68b8f5fa64135d2ca9f2d7 sha1值: 5f837bc434658976cc146e687d5e02fe523de45c sha256值: 23e09e40eeb2875df29c4770f65a3f9e6e12d22a726ade04918efd7fd4329bf7 sha512值: 0cbddd036fe0828005f8465de0ee4a6f85b3f6174ee3ecee8c09fb5b6719cce9ab770810f06ddd8e6cd76f1708e960f011cc846acefc4b2fc2277aeef7d29425 公钥算法: rsa 密钥长度: 2048 指纹: a4e7e9008e72b6f23fcf58e37ad1053137e537bb53994f22454792b0d206138a**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "about\_item\_author\_github" : "联系作者"  |
| "lab\_forget\_password" : "忘记密码?"  |
| "lab\_login\_by\_password" : "密码登录"  |
| "mapbox\_access\_token" : "sk.eyJ1IjoiNDA3MTg1MDMzIiwiYSI6ImNrM3RnODJrNjAyY2szbW8zcDhuc25jcjgifQ.HKwpj5fddwWGUiW6laviBA"  |
| "regex\_password" : "^(?:(?=.\*[a-zA-Z])(?=.\*[0-9])).{8,18}$"  |
| "regex\_user\_name" : "^((13[0-9])|(14[5,7])|(15[0-3,5-9])|(16[6])|(17[0,1,3,5-8])|(18[0-9])|(19[8,9]))\d{8}$"  |
| "tip\_please\_input\_user\_name" : "请输入用户名"  |
| "url\_author\_github" : "https://gitee.com/xuexiangjys/xuexiangjys"  |

## **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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 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 |
| 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\_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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.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.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.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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\_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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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.USES\_POLICY\_FORCE\_LOCK | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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.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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.jinhe.newwanzhang.core.webview.AgentWebActivity | **Schemes**: http://, https://, about://, javascript://, inline://, **Mime Types:** text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml,  |

**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。**