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

**城管通（ 1.5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 | 城管通 |
| 版本 | 1.5 |
| 包名 | com.topevery.supervisor |
| 域名线索 | 57条 |
| URL线索 | 90条 |
| APP图标 |  |
| 分析日期 | 2025年9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 | shantouUrban.apk |
| 文件大小 | 61.6MB |
| MD5值 | 9f2123630f62b115d7699ff9cc4692c7 |
| SHA1值 | 3e91debbb3cdecede58ed4ac2041618a9a0e3309 |
| SHA256值 | e993d54d32c75434d7344a18871ee946ffd89489a9fb981f215cdc05bb19ed5e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 城管通 |
| 包名 | com.topevery.supervisor |
| 主活动Activity | com.topevery.supervisor.ui.SplashActivity |
| 安卓版本名称 | 1.5 |
| 安卓版本 | 5 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ddsdk.vectors.map.qq.com | IP: 109.244.244.164 所属国家: China 地区: Beijing 城市: Beijing  |
| rqd.uu.qq.com | IP: 182.254.88.185 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| 10.101.16.226 | IP: 10.101.16.226 所属国家: - 地区: - 城市: -  |
| oth.eve.mdt.qq.com | IP: 109.244.216.125 所属国家: China 地区: Beijing 城市: Beijing  |
| closedroadvector.map.qq.com | IP: 109.244.244.109 所属国家: China 地区: Beijing 城市: Beijing  |
| ddsdk.vectors2.map.qq.com | IP: 109.244.244.185 所属国家: China 地区: Beijing 城市: Beijing  |
| android.bugly.qq.com | IP: 109.244.244.137 所属国家: China 地区: Beijing 城市: Beijing  |
| vse.baidu.com | IP: 110.242.68.241 所属国家: China 地区: Hebei 城市: Baoding  |
| apilocate.amap.com | IP: 59.82.60.15 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| vop.baidu.com | IP: 111.206.209.68 所属国家: China 地区: Beijing 城市: Beijing  |
| adiu.amap.com | IP: 59.82.31.67 所属国家: China 地区: Beijing 城市: Beijing  |
| yun-hl.3g.qq.com | IP: 175.27.0.142 所属国家: China 地区: Beijing 城市: Beijing  |
| netty.io | IP: 172.67.130.186 所属国家: United States of America 地区: California 城市: San Francisco  |
| vectorsdk.map.qq.com | IP: 109.244.244.164 所属国家: China 地区: Beijing 城市: Beijing  |
| 192.168.20.67 | IP: 192.168.20.67 所属国家: - 地区: - 城市: -  |
| mst01.is.autonavi.com | IP: 106.11.14.3 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| wb.amap.com | IP: 59.82.60.60 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| verify.baidubce.com | IP: 110.242.69.180 所属国家: China 地区: Hebei 城市: Baoding  |
| wap.amap.com | IP: 111.164.19.224 所属国家: China 地区: Tianjin 城市: Tianjin  |
| jrlt.beacon.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| sdkss.shitu.baidu.com | IP: 180.97.33.148 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| tcdnsipv6.myqcloud.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| www.eclipse.org | IP: 198.41.30.198 所属国家: Canada 地区: Ontario 城市: Ottawa  |
| yuyin.baidu.com | IP: 153.3.236.85 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| up-hl.3g.qq.com | IP: 109.244.209.98 所属国家: China 地区: Beijing 城市: Beijing  |
| livepull.myqcloud.com | IP: 14.22.9.178 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| restapi.amap.com | IP: 203.119.175.194 所属国家: China 地区: Beijing 城市: Beijing  |
| overseactrl.map.qq.com | IP: 109.244.173.174 所属国家: China 地区: Beijing 城市: Beijing  |
| yuntuapi.amap.com | 没有服务器地理信息.  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| confinfo.map.qq.com | IP: 175.27.9.21 所属国家: China 地区: Beijing 城市: Beijing  |
| 3891.liveplay.myqcloud.com | IP: 42.81.4.174 所属国家: China 地区: Tianjin 城市: Tianjin  |
| wprd0d.is.autonavi.com | 没有服务器地理信息.  |
| aip.baidubce.com | IP: 111.206.210.12 所属国家: China 地区: Beijing 城市: Beijing  |
| dualstack-a.apilocate.amap.com | IP: 106.11.40.50 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| apiinit.amap.com | IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| restsdk.amap.com | IP: 106.11.43.113 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| tcdns.myqcloud.com | IP: 106.55.123.19 所属国家: China 地区: Beijing 城市: Beijing  |
| m5.amap.com | IP: 106.11.43.74 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| 192.168.20.76 | IP: 192.168.20.76 所属国家: - 地区: - 城市: -  |
| abroad.apilocate.amap.com | IP: 59.82.34.246 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| pr.map.qq.com | IP: 182.254.63.54 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| tafrtt.map.qq.com | IP: 109.244.244.185 所属国家: China 地区: Beijing 城市: Beijing  |
| apikey.map.qq.com | IP: 182.254.57.47 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| dldir1.qq.com | IP: 121.51.177.58 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| upl.baidu.com | IP: 110.242.68.241 所属国家: China 地区: Hebei 城市: Baoding  |
| livepullipv6.myqcloud.com | IP: 119.147.190.45 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| oth.str.mdt.qq.com | IP: 183.36.108.26 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| dualstack-arestapi.amap.com | IP: 39.98.22.142 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| schemas.android.com | 没有服务器地理信息.  |
| mpsapi.amap.com | IP: 203.119.169.143 所属国家: China 地区: Beijing 城市: Beijing  |
| p0.map.gtimg.com | IP: 182.254.54.167 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| lbs.amap.com | IP: 59.82.29.231 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.shantouszcg.top | IP: 183.239.104.155 所属国家: China 地区: Guangdong 城市: Zhanjiang  |
| mapvectors.map.qq.com | IP: 175.27.8.51 所属国家: China 地区: Beijing 城市: Beijing  |
| strategy.beacon.qq.com | IP: 121.51.80.238 所属国家: China 地区: Guangdong 城市: Shenzhen  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt}indent-amount  | com/blankj/utilcode/util/LogUtils.java  |
| http://192.168.20.67:5150/greenGridSys/list  | com/topevery/supervisor/Presenter/GreenbeltPresenter.java  |
| https://10.101.16.226:12443/sqmap/search/solr?start=0&rows=1&x1=  | com/topevery/supervisor/Presenter/AddressServicePresenter.java  |
| http://schemas.android.com/apk/res-auto  | com/topevery/supervisor/ui/view/MenuItemView.java  |
| https://10.101.16.226:12443/api/filesApi/files/  | com/topevery/supervisor/cache/DataCacheManager.java  |
| https://www.shantouszcg.top/api/publicsApi/  | com/topevery/supervisor/entities/ConstantEntity.java  |
| https://www.shantouszcg.top  | com/topevery/supervisor/entities/ConstantEntity.java  |
| http://192.168.20.76:15030/health/addHealth  | com/topevery/supervisor/yq/YqdjActivity.java  |
| http://restapi.amap.com  | com/loc/t.java  |
| http://apilocate.amap.com/mobile/binary  | com/loc/di.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/di.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/db.java  |
| http://abroad.apilocate.amap.com/mobile/binary  | com/loc/Cdo.java  |
| https://adiu.amap.com/ws/device/adius  | com/loc/bl.java  |
| http://restapi.amap.com/v3/geocode/regeo  | com/loc/dd.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/loc/m.java  |
| http://restapi.amap.com/v3/iasdkauth  | com/loc/m.java  |
| http://restapi.amap.com/v3/place/text?  | com/loc/a.java  |
| http://restapi.amap.com/v3/place/around?  | com/loc/a.java  |
| http://restapi.amap.com/v3/config/district?  | com/loc/a.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/beta/upgrade/BetaUploadStrategy.java  |
| http://rqd.uu.qq.com/rqd/sync  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| http://android.bugly.qq.com/rqd/async  | com/tencent/bugly/crashreport/common/strategy/StrategyBean.java  |
| https://github.com/Tencent/tinker/issues  | com/tencent/tinker/lib/reporter/DefaultLoadReporter.java  |
| https://github.com/Tencent/tinker/issues  | com/tencent/tinker/lib/reporter/DefaultPatchReporter.java  |
| http://%s/timeshift/%s/%s/timeshift.m3u8?delay=%d  | com/tencent/liteav/j.java  |
| http://%s/%s/%s/timeshift.m3u8?starttime=%s&appid=%s&txKbps=0  | com/tencent/liteav/j.java  |
| http://%s/timeshift/%s/%s/timeshift.m3u8?delay=0  | com/tencent/liteav/j.java  |
| http://%s/%s/%s/timeshift.m3u8?delay=0&appid=%s&txKbps=0  | com/tencent/liteav/j.java  |
| http://3891.liveplay.myqcloud.com/live/  | com/tencent/liteav/demo/trtc/TRTCMainActivity.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_boomAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_nihongshuAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_starearAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_fengkuangdacallAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_QxingzuoAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_caidaiAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_liuhaifadaiAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_lianpuAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_purplecatAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_huaxianziAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_baby\_agetestAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| http://dldir1.qq.com/hudongzhibo/AISpecial/Android/170/video\_xiaofuAndroid.zip  | com/tencent/liteav/demo/trtc/widget/TRTCBeautySettingPanel.java  |
| https://livepull.myqcloud.com/getpulladdr  | com/tencent/liteav/network/h.java  |
| https://livepullipv6.myqcloud.com/getpulladdr  | com/tencent/liteav/network/h.java  |
| https://tcdns.myqcloud.com/queryip  | com/tencent/liteav/network/c.java  |
| https://tcdnsipv6.myqcloud.com/queryip  | com/tencent/liteav/network/c.java  |
| https://vectorsdk.map.qq.com  | com/tencent/tencentmap/net/a.java  |
| https://tafrtt.map.qq.com/rttserverex/  | com/tencent/tencentmap/net/a.java  |
| https://vectorsdk.map.qq.com  | com/tencent/tencentmap/config/ConfigFileDownloader.java  |
| https://p0.map.gtimg.com/scenic/  | com/tencent/tencentmap/mapsdk/maps/a/js.java  |
| http://strategy.beacon.qq.com/analytics/upload?mType=beacon  | com/tencent/tencentmap/mapsdk/maps/a/bf.java  |
| https://overseactrl.map.qq.com/?  | com/tencent/tencentmap/mapsdk/maps/a/jm.java  |
| https://apikey.map.qq.com/mkey/index.php/mkey/check?key=%s&pid=%s&key2=%s&pid2=%s&channel=1&output=json&uuid=unknown&hm=%s&suid=%s&os=%s&psv=%s&ver=%s&dpi=%s&pf=%s&nt=%s  | com/tencent/tencentmap/mapsdk/maps/a/ic.java  |
| https://up-hl.3g.qq.com/upreport  | com/tencent/tencentmap/mapsdk/maps/a/cy.java  |
| https://yun-hl.3g.qq.com/halleycloud  | com/tencent/tencentmap/mapsdk/maps/a/ej.java  |
| http://oth.str.mdt.qq.com:8080/analytics/upload  | com/tencent/tencentmap/mapsdk/maps/a/v.java  |
| http://oth.eve.mdt.qq.com:8080/analytics/upload  | com/tencent/tencentmap/mapsdk/maps/a/v.java  |
| http://jrlt.beacon.qq.com/analytics/upload  | com/tencent/tencentmap/mapsdk/maps/a/v.java  |
| https://confinfo.map.qq.com/confinfo?  | com/tencent/tencentmap/mapsdk/maps/a/jt.java  |
| https://closedroadvector.map.qq.com/closed\_road\_v2?  | com/tencent/tencentmap/mapsdk/maps/a/jf.java  |
| https://p0.map.gtimg.com/scenic/  | com/tencent/tencentmap/mapsdk/maps/a/jf.java  |
| https://ddsdk.vectors.map.qq.com  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://ddsdk.vectors2.map.qq.com  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://mapvectors.map.qq.com  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://vectorsdk.map.qq.com  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://vectorsdk.map.qq.com/indoor\_map?  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://mapvectors.map.qq.com/indoormap2?  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://closedroadvector.map.qq.com/closed\_road\_v2?  | com/tencent/tencentmap/mapsdk/maps/a/hs.java  |
| https://pr.map.qq.com/pingd?  | com/tencent/tencentmap/mapsdk/maps/a/ls.java  |
| https://tafrtt.map.qq.com/rttserverex/  | com/tencent/tencentmap/mapsdk/maps/a/il.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  |
| http://sdkss.shitu.baidu.com/cgi-bin/sdkstat.py  | com/baidu/idl/statistics/Statistics.java  |
| http://sdkss.shitu.baidu.com/cgi-bin/queryLicense.py  | com/baidu/idl/license/License.java  |
| https://vse.baidu.com/v2  | com/baidu/speech/asr/SpeechConstant.java  |
| https://vse.baidu.com/echo.fcgi  | com/baidu/speech/asr/SpeechConstant.java  |
| https://upl.baidu.com//words/add  | com/baidu/speech/asr/SlotControl.java  |
| http://yuyin.baidu.com/voice?osname=voiceopen&action=usereventflow&  | com/baidu/speech/utils/analysis/Analysis.java  |
| http://vop.baidu.com/v2  | com/baidu/speech/core/ASREngine.java  |
| http://mpsapi.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.java  |
| http://m5.amap.com/  | com/autonavi/base/ae/gmap/GLMapEngine.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://m5.amap.com/  | com/autonavi/base/amap/mapcore/maploader/AMapLoader.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明  | com/autonavi/amap/mapcore/Inner\_3dMap\_location.java  |
| http://schemas.android.com/apk/res/android  | com/xuexiang/xui/widget/banner/widget/banner/base/BaseBanner.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/services/a/bi.java  |
| https://restapi.amap.com/v3/iasdkauth  | com/amap/api/services/a/bh.java  |
| http://restapi.amap.com/v3/iasdkauth  | com/amap/api/services/a/bh.java  |
| http://wb.amap.com/?r=%f,%f,%s,%f,%f,%s,%d,%d,%d,%s,%s,%s&sourceapplication=openapi/0  | com/amap/api/services/a/bb.java  |
| http://wb.amap.com/?q=%f,%f,%s&sourceapplication=openapi/0  | com/amap/api/services/a/bb.java  |
| http://wb.amap.com/?n=%f,%f,%f,%f,%d&sourceapplication=openapi/0  | com/amap/api/services/a/bb.java  |
| http://wb.amap.com/?p=%s,%f,%f,%s,%s&sourceapplication=openapi/0  | com/amap/api/services/a/bb.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/services/a/de.java  |
| http://restapi.amap.com  | com/amap/api/services/a/bo.java  |
| http://restapi.amap.com/v3  | com/amap/api/services/a/i.java  |
| https://restapi.amap.com/v3  | com/amap/api/services/a/i.java  |
| http://restapi.amap.com/v4  | com/amap/api/services/a/i.java  |
| https://restapi.amap.com/v4  | com/amap/api/services/a/i.java  |
| http://yuntuapi.amap.com  | com/amap/api/services/a/i.java  |
| https://yuntuapi.amap.com  | com/amap/api/services/a/i.java  |
| http://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/services/a/i.java  |
| https://m5.amap.com/ws/mapapi/shortaddress/transform  | com/amap/api/services/a/i.java  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | com/amap/api/mapcore/util/b.java  |
| https://restsdk.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| https://dualstack-arestapi.amap.com/v3/iasdkauth  | com/amap/api/mapcore/util/ew.java  |
| https://adiu.amap.com/ws/device/adius  | com/amap/api/mapcore/util/gv.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/ct.java  |
| http://restsdk.amap.com/v4/grasproad/driving?  | com/amap/api/mapcore/util/eq.java  |
| http://wprd0%d.is.autonavi.com/appmaptile?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com/v4/gridmap?  | com/amap/api/mapcore/util/cs.java  |
| http://restsdk.amap.com  | com/amap/api/mapcore/util/fe.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/cf.java  |
| http://restsdk.amap.com/v4  | com/amap/api/mapcore/util/i.java  |
| http://apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://dualstack-a.apilocate.amap.com/mobile/binary  | com/amap/api/mapcore/util/io.java  |
| http://apiinit.amap.com/v3/log/init  | com/amap/api/mapcore/util/ex.java  |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明  | com/amap/api/location/AMapLocation.java  |
| http://wap.amap.com/  | com/amap/api/maps/AMapUtils.java  |
| http://xml.apache.org/xslt}indent-amount  | com/orhanobut/logger/LoggerPrinter.java  |
| http://netty.io/wiki/reference-counted-objects.html  | io/netty/util/ResourceLeakDetector.java  |
| http://netty.io/wiki/forked-tomcat-native.html  | io/netty/handler/ssl/OpenSsl.java  |
| http://www.eclipse.org/jetty/documentation/current/npn-chapter.html#npn-starting  | io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java  |
| http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html#alpn-starting  | io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java  |
| https://github.com/vinc3m1  | Android String Resource  |
| https://github.com/vinc3m1/RoundedImageView  | Android String Resource  |
| https://github.com/vinc3m1/RoundedImageView.git  | Android String Resource  |
| http://mpsapi.amap.com/ws/mps/vmap  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/rtt  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/smap  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mpsapi.amap.com/  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://m5.amap.com  | lib/armeabi/libAMapSDK\_MAP\_v8\_0\_0.so  |
| http://mapvectors.map.qq.com  | lib/armeabi/libtxmapengine.so  |
| http://p0.map.gtimg.com/sateTiles/%d/%d/%d/%d\_%d.jpg  | lib/armeabi/libtxmapengine.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| poi\_icon@2x.png poi\_icon\_nav@2x.png poi\_icon\_dark@2x.png poi\_icon\_indoor@2x.png  | com/tencent/tencentmap/mapsdk/maps/a/jn.java  |
| poi\_icon\_indoor@2x.png  | com/tencent/tencentmap/mapsdk/maps/a/jo.java  |
| jrs@cs.berkeley  | lib/armeabi/libtxmapengine.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 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  |
| 18142669622  | com/topevery/supervisor/ui/ContactsActivity.java  |

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=86, ST=gd, L=sz, O=topevery, OU=topevery, CN=eric.xu Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2011-07-01 06:42:49+00:00 Valid To: 2066-04-03 06:42:49+00:00 Issuer: C=86, ST=gd, L=sz, O=topevery, OU=topevery, CN=eric.xu Serial Number: 0x4e0d6c69 Hash Algorithm: sha1 md5: 094841be029ee3ff8fe8deace8ed6fac sha1: 5a0f766247c6686f93d97233d6412fb50f999e67 sha256: cd77fbfb198d02b12deb209beb6b39c960f5ea98b008704ef5bb4d329af1d6a0 sha512: e1e5227d098f867edfa81e85b5aae3da92feb14ab42014465c8495d21ad2bde7b0108f7cad658ff076707ffc87b46939c877e350faff8a24f413533354004b61 PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: fb338aa9cb7b8f9e5fab41909283253feaa56ce7f0e51e6269c6330693c4fcfb**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "Please\_enter\_a\_username" : "Please enter a username"  |
| "Two\_input\_password" : "Inconsistent password, please enter again!"  |
| "biometric\_dialog\_use\_password" : "使用密码"  |
| "illegal\_user\_name" : "Illegal user name"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "password" : "Password"  |
| "session" : "Conversation"  |
| "user\_name" : "User name"  |

## **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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.READ\_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\_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\_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.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.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.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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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 |

## **10. 应用内通信**

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