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

**元道经纬相机（ 3.2.1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 | 元道经纬相机 |
| 版本 | 3.2.1 |
| 包名 | com.ydtx.camera |
| 域名线索 | 42条 |
| URL线索 | 41条 |
| APP图标 |  |
| 分析日期 | 2025年6月19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 | 元道经纬相机.apk |
| 文件大小 | 13.37MB |
| MD5值 | e649c7121862e6fe0dc81568e448cc3c |
| SHA1值 | b452343634f8c9b9140ec4f6a3e446d4d612de56 |
| SHA256值 | 671ba41551f2c2d11e9685fa14bc3d21eb92e68ef3f7a909e0dc64ed6d11963e |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 元道经纬相机 |
| 包名 | com.ydtx.camera |
| 主活动Activity | com.ydtx.camera.SplashActivity |
| 安卓版本名称 | 3.2.1 |
| 安卓版本 | 37 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ulogs.umengcloud.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| plbslog.umeng.com.gds.alibabadns.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| alogsus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| api.map.baidu.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| www.jd.com | IP: 116.78.120.73 所属国家: China 地区: Beijing 城市: Beijing  |
| www.taobao.com | IP: 101.72.202.200 所属国家: China 地区: Hebei 城市: Langfang  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ofloc.map.baidu.com | IP: 111.206.209.193 所属国家: China 地区: Beijing 城市: Beijing  |
| j.map.baidu.com | IP: 111.206.209.187 所属国家: China 地区: Beijing 城市: Beijing  |
| cmnsguider.yunos.com | IP: 203.119.145.40 所属国家: China 地区: Beijing 城市: Beijing  |
| itsdata.map.baidu.com | IP: 111.206.209.180 所属国家: China 地区: Beijing 城市: Beijing  |
| dualstack-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com | IP: 203.119.213.102 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ulogs.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| loc.map.baidu.com | IP: 111.206.209.175 所属国家: China 地区: Beijing 城市: Beijing  |
| www.baidu.com | IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| bbs.lbsyun.baidu.com | 没有服务器地理信息.  |
| daohang.map.baidu.com | IP: 111.206.209.190 所属国家: China 地区: Beijing 城市: Beijing  |
| app.navi.baidu.com | IP: 111.206.209.213 所属国家: China 地区: Beijing 城市: Beijing  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| alogus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| client.map.baidu.com | IP: 111.206.209.120 所属国家: China 地区: Beijing 城市: Beijing  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.360.cn | IP: 101.199.254.116 所属国家: China 地区: Beijing 城市: Beijing  |
| creativecommons.org | IP: 104.20.5.134 所属国家: United States of America 地区: California 城市: San Francisco  |
| bjsmms.wintaotel.com.cn | IP: 121.201.107.181 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| api.map.n.shifen.com | IP: 111.206.208.72 所属国家: China 地区: Beijing 城市: Beijing  |
| shortvideo.qiniuapi.com | IP: 121.52.255.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| c.tenor.com | IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco  |
| connectivitycheck.gstatic.com | IP: 203.208.43.98 所属国家: China 地区: Beijing 城市: Beijing  |
| wapmap.baidu.com | IP: 111.206.209.212 所属国家: China 地区: Beijing 城市: Beijing  |
| googlehosted.l.googleusercontent.com | IP: 173.194.203.132 所属国家: United States of America 地区: California 城市: Mountain View  |
| t.weather.itboy.net | IP: 61.48.83.207 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umeng.com.gds.alibabadns.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.gstatic.com | IP: 203.208.43.98 所属国家: China 地区: Beijing 城市: Beijing  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| map.baidu.com | IP: 111.206.208.32 所属国家: China 地区: Beijing 城市: Beijing  |
| daup.map.baidu.com | IP: 110.242.74.236 所属国家: China 地区: Hebei 城市: Baoding  |
| media.tenor.com | IP: 103.226.246.99 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.ntsc.ac.cn | IP: 159.226.242.43 所属国家: China 地区: Beijing 城市: Beijing  |
| alogus.umeng.com.gds.alibabadns.com | IP: 223.109.148.178 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| zyxj.wintaotel.com.cn | 没有服务器地理信息.  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://api.map.baidu.com/sdkcs/verify  | com/baidu/lbsapi/auth/LBSAuthManager.java  |
| https://api.map.baidu.com/geosearch/v2/detail/  | com/baidu/mapapi/cloud/DetailSearchInfo.java  |
| http://api.map.baidu.com/geosearch/v2/detail/  | com/baidu/mapapi/cloud/DetailSearchInfo.java  |
| https://api.map.baidu.com/geosearch/v2/local  | com/baidu/mapapi/cloud/LocalSearchInfo.java  |
| http://api.map.baidu.com/geosearch/v2/local  | com/baidu/mapapi/cloud/LocalSearchInfo.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1  | com/baidu/mapapi/cloud/CloudRgcInfo.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1  | com/baidu/mapapi/cloud/CloudRgcInfo.java  |
| https://api.map.baidu.com/geosearch/v2/nearby  | com/baidu/mapapi/cloud/NearbySearchInfo.java  |
| http://api.map.baidu.com/geosearch/v2/nearby  | com/baidu/mapapi/cloud/NearbySearchInfo.java  |
| https://api.map.baidu.com/geosearch/v2/bound  | com/baidu/mapapi/cloud/BoundSearchInfo.java  |
| http://api.map.baidu.com/geosearch/v2/bound  | com/baidu/mapapi/cloud/BoundSearchInfo.java  |
| http://app.navi.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://daohang.map.baidu.com/mobile/  | com/baidu/mapapi/navi/BaiduMapNavigation.java  |
| http://map.baidu.com/zt/client/index/?fr=sdk\_[  | com/baidu/mapapi/utils/OpenClientUtil.java  |
| http://api.map.baidu.com/place/detail?uid=  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/place/search?  | com/baidu/mapapi/utils/poi/BaiduMapPoiSearch.java  |
| http://api.map.baidu.com/direction?  | com/baidu/mapapi/utils/route/BaiduMapRoutePlan.java  |
| http://loc.map.baidu.com/iofd.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/wloc  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/sdk.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/user\_err.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/oqur.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/tcu.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/rtbu.php  | com/baidu/location/h/j.java  |
| http://loc.map.baidu.com/sdk\_ep.php  | com/baidu/location/h/j.java  |
| https://loc.map.baidu.com/sdk.php  | com/baidu/location/h/j.java  |
| https://daup.map.baidu.com/cltr/rcvr  | com/baidu/location/h/j.java  |
| http://itsdata.map.baidu.com/long-conn-gps/sdk.php  | com/baidu/location/a/f.java  |
| http://loc.map.baidu.com/cc.php  | com/baidu/location/a/d.java  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | com/baidu/location/c/a.java  |
| http://loc.map.baidu.com/apigetindoordata.php  | com/baidu/location/c/a/a.java  |
| http://loc.map.baidu.com/gpsz  | com/baidu/location/b/a.java  |
| http://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/h.java  |
| http://%s/%s  | com/baidu/location/e/d.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/d.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/k.java  |
| https://ofloc.map.baidu.com/offline\_loc  | com/baidu/location/e/g.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/RadarService/  | com/baidu/platform/comapi/radar/c.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/RadarService/  | com/baidu/platform/comapi/radar/c.java  |
| http://bbs.lbsyun.baidu.com/forum.php?mod=viewthread&tid=106461\n=============================================\n  | com/baidu/platform/comapi/util/PermissionCheck.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkws/place/v2/detail  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui/v1/  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/a.java  |
| http://j.map.baidu.com/  | com/baidu/platform/domain/a.java  |
| http://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/a.java  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/a.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkws/place/v2/detail  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui/v1/  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | com/baidu/platform/domain/b.java  |
| https://j.map.baidu.com/  | com/baidu/platform/domain/b.java  |
| https://client.map.baidu.com/imap/share/ps  | com/baidu/platform/domain/b.java  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | com/baidu/platform/domain/b.java  |
| http://wapmap.baidu.com/s?tn=Detail&pid=  | com/baidu/platform/core/e/c.java  |
| http://map.baidu.com/?newmap=1&s=  | com/baidu/platform/core/e/e.java  |
| https://shortvideo.qiniuapi.com/v1/status/a  | com/qiniu/pili/droid/shortvideo/b/g.java  |
| https://shortvideo.qiniuapi.com/v1/zeus?appid=  | com/qiniu/pili/droid/shortvideo/b/u.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://ulogs.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com/unify\_logs  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://cmnsguider.yunos.com:443/genDeviceToken  | com/umeng/commonsdk/statistics/idtracking/s.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/h.java  |
| http://zyxj.wintaotel.com.cn/CommController/showImg?imgPath=  | com/ydtx/camera/BigImageViewActivity.java  |
| http://zyxj.wintaotel.com.cn//WMCameraController/authorizeForAndroid  | com/ydtx/camera/SplashActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/getFileFolder  | com/ydtx/camera/UpFileActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/downloadFile  | com/ydtx/camera/UpFileActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/uploadFile  | com/ydtx/camera/UpFileActivity.java  |
| http://zyxj.wintaotel.com.cn//WMCameraController/insertDataForAndroid  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/login  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/register.jsp  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/logout  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/editPassword  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/getFileFolder  | com/ydtx/camera/MainActivity.java  |
| http://www.baidu.com  | com/ydtx/camera/MainActivity.java  |
| http://www.ntsc.ac.cn  | com/ydtx/camera/MainActivity.java  |
| http://www.taobao.com  | com/ydtx/camera/MainActivity.java  |
| http://www.jd.com  | com/ydtx/camera/MainActivity.java  |
| https://www.360.cn/  | com/ydtx/camera/MainActivity.java  |
| http://t.weather.itboy.net/api/weather/city/  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/uploadFile  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/getOrgLogo  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/downloadOrgLogo  | com/ydtx/camera/MainActivity.java  |
| http://zyxj.wintaotel.com.cn/  | com/ydtx/camera/utils/Util.java  |
| http://bjsmms.wintaotel.com.cn/pipeline/camerainterfaceAction!updateVersion?  | com/ydtx/camera/utils/Util.java  |
| http://bjsmms.wintaotel.com.cn/camera/cameraAction!loadAndMaxVersion?  | com/ydtx/camera/utils/Util.java  |
| http://bjsmms.wintaotel.com.cn/upload  | com/ydtx/camera/utils/Util.java  |
| http://www.baidu.com  | com/ydtx/camera/utils/Util.java  |
| http://api.map.baidu.com/geocoder/v2/  | com/ydtx/camera/utils/Util.java  |
| http://zyxj.wintaotel.com.cn/CommController/showImg?imgPath=  | com/ydtx/camera/adapter/DownloadFileListAdapter.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/downloadFile  | com/ydtx/camera/Service/DownloadService.java  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/uploadFile  | com/ydtx/camera/Service/DownloadService.java  |
| http://bjsmms.wintaotel.com.cn/pipeline/camerainterfaceAction  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | 摸瓜V3引擎  |
| api.map.baidu.com  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | 摸瓜V3引擎  |
| instantmessaging-pa.googleapis.com  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/transit  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/CommController/showImg?imgPath=  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/editPassword  | 摸瓜V3引擎  |
| dualstack-na61-na62.wagbridge.alibaba.tanx.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| alogus.umeng.com  | 摸瓜V3引擎  |
| https://api.map.baidu.com/geosearch/v2/bound  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| https://api.map.baidu.com/geosearch/v2/detail/  | 摸瓜V3引擎  |
| http://api.map.baidu.com/geocoder/v2/  | 摸瓜V3引擎  |
| http://creativecommons.org/licenses/publicdomain  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/s  | 摸瓜V3引擎  |
| http://api.map.baidu.com/geosearch/v2/detail/  | 摸瓜V3引擎  |
| http://bjsmms.wintaotel.com.cn/camera/cameraAction  | 摸瓜V3引擎  |
| https://www.360.cn/  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkws/place/v2/detail  | 摸瓜V3引擎  |
| https://developer.umeng.com/docs/66632/detail/  | 摸瓜V3引擎  |
| www.gstatic.com  | 摸瓜V3引擎  |
| plbslog.umeng.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| media.tenor.com  | 摸瓜V3引擎  |
| http://loc.map.baidu.com/cc.php  | 摸瓜V3引擎  |
| https://shortvideo.qiniuapi.com/v1/zeus?appid=  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | 摸瓜V3引擎  |
| https://ofloc.map.baidu.com/offline\_loc  | 摸瓜V3引擎  |
| https://j.map.baidu.com/  | 摸瓜V3引擎  |
| ulogs.umeng.com  | 摸瓜V3引擎  |
| http://www.baidu.com  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui/v1/  | 摸瓜V3引擎  |
| http://itsdata.map.baidu.com/long-conn-gps/sdk.php  | 摸瓜V3引擎  |
| http://loc.map.baidu.com/indoorlocbuildinginfo.php  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/login  | 摸瓜V3引擎  |
| http://loc.map.baidu.com/gpsz  | 摸瓜V3引擎  |
| c.tenor.com  | 摸瓜V3引擎  |
| android.googleapis.com  | 摸瓜V3引擎  |
| http://www.jd.com  | 摸瓜V3引擎  |
| http://t.weather.itboy.net/api/weather/city/  | 摸瓜V3引擎  |
| googlehosted.l.googleusercontent.com  | 摸瓜V3引擎  |
| https://api.map.baidu.com/geosearch/v2/nearby  | 摸瓜V3引擎  |
| https://client.map.baidu.com/imap/share/ps  | 摸瓜V3引擎  |
| https://github.com/nostra13/Android-Universal-Image-Loader/issues/376  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/place/v2/suggestion  | 摸瓜V3引擎  |
| clientservices.googleapis.com  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/getOrgLogo  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/register.jsp  | 摸瓜V3引擎  |
| zyxj.wintaotel.com.cn  | 摸瓜V3引擎  |
| ulogs.umengcloud.com  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | 摸瓜V3引擎  |
| http://client.map.baidu.com/imap/share/ps  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/getFileFolder  | 摸瓜V3引擎  |
| http://loc.map.baidu.com/apigetindoordata.php  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | 摸瓜V3引擎  |
| gmscompliance-pa.googleapis.com  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/logout  | 摸瓜V3引擎  |
| http://www.ntsc.ac.cn  | 摸瓜V3引擎  |
| ulogs.umeng.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkcs/verify  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/pathplan/v2/riding  | 摸瓜V3引擎  |
| alogus.umeng.com.gds.alibabadns.com  | 摸瓜V3引擎  |
| api.map.n.shifen.com  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/apimap/v1/  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/cloudrgc/v1  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | 摸瓜V3引擎  |
| http://j.map.baidu.com/  | 摸瓜V3引擎  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/downloadOrgLogo  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/indoor/v1/  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui2/v1/  | 摸瓜V3引擎  |
| https://shortvideo.qiniuapi.com/v1/status/a  | 摸瓜V3引擎  |
| http://api.map.baidu.com/sdkws/place/v2/detail  | 摸瓜V3引擎  |
| growth-pa.googleapis.com  | 摸瓜V3引擎  |
| http://map.baidu.com/?newmap=1&s=  | 摸瓜V3引擎  |
| http://www.taobao.com  | 摸瓜V3引擎  |
| connectivitycheck.gstatic.com  | 摸瓜V3引擎  |
| http://api.map.baidu.com/geosearch/v2/bound  | 摸瓜V3引擎  |
| http://bjsmms.wintaotel.com.cn/upload  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/downloadFile  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/lbs\_androidsdk/phpui/v1/  | 摸瓜V3引擎  |
| http://ofloc.map.baidu.com/offline\_loc  | 摸瓜V3引擎  |
| http://api.map.baidu.com/geosearch/v2/nearby  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn//WMCameraController/authorizeForAndroid  | 摸瓜V3引擎  |
| https://api.map.baidu.com/geosearch/v2/local  | 摸瓜V3引擎  |
| http://developer.umeng.com/docs/66650/cate/66650  | 摸瓜V3引擎  |
| https://api.map.baidu.com/sdkproxy/v2/lbs\_androidsdk/geocoder/v2  | 摸瓜V3引擎  |
| http://api.map.baidu.com/geosearch/v2/local  | 摸瓜V3引擎  |
| http://wapmap.baidu.com/s?tn=Detail&pid=  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn/AndroidClientInterface/uploadFile  | 摸瓜V3引擎  |
| plbslog.umeng.com  | 摸瓜V3引擎  |
| http://zyxj.wintaotel.com.cn//WMCameraController/insertDataForAndroid  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 18345352118  | com/baidu/platform/comapi/util/b.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=aa, ST=aa, L=aa, O=aa, OU=aa, CN=aa 签名算法: rsassa\_pkcs1v15 有效期自: 2014-11-26 08:42:21+00:00 有效期至: 2064-11-13 08:42:21+00:00 发行人: C=aa, ST=aa, L=aa, O=aa, OU=aa, CN=aa 序列号: 0x5475926d 哈希算法: sha1 md5值: 9141ea7ed989ad0f66a4782a2a565696 sha1值: c31072a9afb5c1b99a23383ab486edcbf6d3cc15 sha256值: 1df25923f1c092a2451cc92e6fefa89a8a688c5abba307d3f293be71f870359e sha512值: e3cc26278a6e2c85135691f89ceee5078b6b5edc432b25890e01ab0f4d9c6a59095141df1c10a9f9358c835016cb930598d330621108870e6220601047ad631a 公钥算法: rsa 密钥长度: 1024 指纹: 489b5893c6cea4573b1b18273bcd2df3901e2ae6c75ad3a69beb0d1cf746c65d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "authorization\_cecks" : "我已阅读并同意此协议!"  |
| "authorization\_protocol\_five" : "7.深圳市元道通信技术有限公司是该产品版权实际拥有者，负责对该产品所有细则及其他信息进行解释。"  |
| "authorization\_protocol\_four" : "5.禁止反向工程、反向编译和反向汇编：用户不得对本软件产品进行反向工程（ReverseEngineer）、反向编译（Decompile）或反向汇编（Disassemble），同时不得改动编译在程序文件内部的任何资源。除法律、法规明文规定允许上述活动外，用户必须遵守此协议限制。"  |
| "authorization\_protocol\_last" : "1.请你认真阅读完《元道经纬相机》服务条款。"  |
| "authorization\_protocol\_one" : "2.本产品为深圳市元道技术有限公司独立开发，深圳市元道通信技术有限公司，拥有该产品一切产权。任何组织、个人未经深圳市元道通信技术有限公司允许，不得盗用此产品。"  |
| "authorization\_protocol\_seven" : "6.为监测软件在使用中出现的bug，软件加入友盟后台统计功能。"  |
| "authorization\_protocol\_three" : "4.使用此产品可对照片进行经纬度及其他信息加载水印，该产品在后续更新过程中将增加多种水印加载模本，深圳市元道通信技术有限公司是该产品外观、相关程序、水印模板等版权拥有者。"  |
| "authorization\_protocol\_two" : "3.禁止将此产品用于非法用途，如因用户个人原因，将此产品用于非法用途，我司将不承担任何法律责任。"  |
| "authorization\_title" : "欢迎使用元道经纬相机"  |

## **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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.READ\_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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |

## **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。**