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

**皖美自然（ 1.1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 | 皖美自然 |
| 版本 | 1.1 |
| 包名 | com.geoway.cloudquery |
| 域名线索 | 68条 |
| URL线索 | 54条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | 皖美自然1.1.apk |
| 文件大小 | 49.77MB |
| MD5值 | 575cc17be3d7ba468f322b3d42045f8e |
| SHA1值 | 25c7f3cc668c8563391406007abd84e4817f450c |
| SHA256值 | f7e4e6e0b5b5fe1c8e1a3936e177fffb89112cd559922592c0fed4747c6b5757 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 皖美自然 |
| 包名 | com.geoway.cloudquery |
| 主活动Activity | com.geoway.cloudquery.web.WebMainActivity |
| 安卓版本名称 | 1.1 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.tianditu.com | IP: 117.78.24.34  所属国家: China  地区: Beijing  城市: Beijing |
| apilocate.amap.com | IP: 59.82.31.183  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gisanalysis.org | 没有服务器地理信息. |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| t1.tianditu.gov.cn | IP: 49.4.56.37  所属国家: China  地区: Beijing  城市: Beijing |
| 172.16.67.34 | IP: 172.16.67.34  所属国家: -  地区: -  城市: - |
| dualstack-arestapi.amap.com | IP: 203.119.169.174  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cfg.imtt.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| download.tianditu.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 |
| www.andykhan.com | IP: 213.171.195.105  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Gloucester |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.232  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: Beijing  城市: Beijing |
| restapi.amap.com | IP: 106.11.43.113  所属国家: China  地区: Beijing  城市: Beijing |
| api.cellocation.com | IP: 43.143.208.149  所属国家: China  地区: Beijing  城市: Beijing |
| www.landcloud.org.cn | IP: 116.205.71.7  所属国家: China  地区: Guangdong  城市: Guangzhou |
| webst04.is.autonavi.com | IP: 122.156.129.75  所属国家: China  地区: Heilongjiang  城市: Heihe |
| log.tbs.qq.com | IP: 124.95.231.218  所属国家: China  地区: Liaoning  城市: Shenyang |
| www.google.cn | IP: 114.250.69.34  所属国家: China  地区: Beijing  城市: Beijing |
| qd.myapp.com | IP: 119.176.28.212  所属国家: China  地区: Shandong  城市: Weifang |
| gss0.bdstatic.com | IP: 61.163.9.31  所属国家: China  地区: Henan  城市: Luoyang |
| 192.168.199.230 | IP: 192.168.199.230  所属国家: -  地区: -  城市: - |
| t0.tianditu.com | IP: 49.4.56.29  所属国家: China  地区: Beijing  城市: Beijing |
| vip.cellocation.com | IP: 82.157.171.80  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: - |
| xmlpull.org | IP: 185.199.108.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.openmobilealliance.org | IP: 104.26.8.105  所属国家: United States of America  地区: California  城市: San Francisco |
| mobsv3.tianditu.com | 没有服务器地理信息. |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| mobile.tianditu.com | 没有服务器地理信息. |
| pms.mb.qq.com | IP: 60.29.240.17  所属国家: China  地区: Tianjin  城市: Tianjin |
| api.map.baidu.com | IP: 111.206.208.72  所属国家: China  地区: Beijing  城市: Beijing |
| t6.tianditu.gov.cn | IP: 49.4.56.32  所属国家: China  地区: Beijing  城市: Beijing |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| tbsrecovery.imtt.qq.com | IP: 61.181.204.91  所属国家: China  地区: Tianjin  城市: Tianjin |
| image.cnamedomain.com | 没有服务器地理信息. |
| t6.tianditu.com | IP: 49.4.56.28  所属国家: China  地区: Beijing  城市: Beijing |
| api.tianditu.gov.cn | IP: 116.205.70.90  所属国家: China  地区: Guangdong  城市: Guangzhou |
| www.wireless-village.org | IP: 172.67.131.214  所属国家: United States of America  地区: California  城市: San Francisco |
| www.googleapis.com | IP: 142.250.217.106  所属国家: United States of America  地区: California  城市: Mountain View |
| 192.168.250.3 | IP: 192.168.250.3  所属国家: -  地区: -  城市: - |
| www.tianditu.cn | IP: 117.78.24.40  所属国家: China  地区: Beijing  城市: Beijing |
| cgicol.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| 192.168.253.67 | IP: 192.168.253.67  所属国家: -  地区: -  城市: - |
| www.opengis.net | IP: 217.154.231.107  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Brighton |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| ditu.zjzwfw.gov.cn | IP: 110.249.209.200  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| www.amazon.co.uk | IP: 3.164.118.50  所属国家: United States of America  地区: Washington  城市: Seattle |
| 118.178.118.177 | IP: 118.178.118.177  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| adiu.amap.com | IP: 110.253.189.146  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| lbs.amap.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| console.tianditu.gov.cn | IP: 116.205.70.147  所属国家: China  地区: Guangdong  城市: Guangzhou |
| webrd01.is.autonavi.com | IP: 101.72.238.92  所属国家: China  地区: Hebei  城市: Langfang |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| www.chinapop.gov.cn | 没有服务器地理信息. |
| 192.168.253.31 | IP: 192.168.253.31  所属国家: -  地区: -  城市: - |
| mns.cn-.aliyuncs.com | 没有服务器地理信息. |
| schemas.xmlsoap.org | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.webxml.com.cn | IP: 61.147.124.120  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| t6.tianditu.cn | 没有服务器地理信息. |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| 192.168.253.25 | IP: 192.168.253.25  所属国家: -  地区: -  城市: - |
| mns.aliyuncs.com | 没有服务器地理信息. |
| maps.ynmap.cn | IP: 182.247.253.70  所属国家: China  地区: Yunnan  城市: Kunming |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| 192.168.253.40 | IP: 192.168.253.40  所属国家: -  地区: -  城市: - |
| dev.dcloud.net.cn | IP: 101.72.227.61  所属国家: China  地区: Hebei  城市: Langfang |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://192.168.250.3/servlet/UploadFile | cn/ajsoft/mywebview/client/OfficeEventListenerImpl.java |
| http://mns.cn-\*\*\*\*.aliyuncs.com'! | com/alibaba/sdk/android/mns/MNSClient.java |
| http://mns.aliyuncs.com/doc/v1 | com/alibaba/sdk/android/mns/common/MNSConstants.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSClient.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSClient.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| https://qd.myapp.com/myapp/qqteam/AndroidQQ/mobileqq\_android.apk | com/geoway/cloudquery/SplashActivity.java |
| http://%s:%d | com/geoway/cloudquery/util/NetworkUtil.java |
| http://gisAnalysis.org/ | com/geoway/cloudquery/util/WebServiceUtils.java |
| http://192.168.253.40:80/AHService\_KJ/DZZH\_Search\_dj.asmx | com/geoway/cloudquery/util/WebServiceUtils.java |
| http://192.168.253.40:80/AHService/DZZH\_Search\_dj.asmx | com/geoway/cloudquery/util/WebServiceUtils.java |
| http://www.webxml.com.cn/WebServices/WeatherWebService.asmx | com/geoway/cloudquery/util/WebServiceUtils.java |
| http://192.168.253.67:9995 | com/geoway/cloudquery/web/WebMainActivity.java |
| https://) | com/geoway/cloudquery/web/WebSettingActivity.java |
| http://api.tianditu.gov.cn/search?tk=%s&postStr= | com/geoway/cloudquery/net/NetBaseContanst.java |
| http://192.168.199.230/AHService/WebForm1.aspx?kjfw= | com/geoway/cloudquery/net/OkhttpUtils.java |
| http://192.168.253.31/index\_dz.jsp?choice= | com/geoway/cloudquery/adapter/ItemOtherCloudServiceAdapter.java |
| http://api.map.baidu.com/geoconv/v1/?coords= | com/geoway/cloudquery/app/SurveyLogic.java |
| http://restapi.amap.com/v3/assistant/coordinate/convert?key=ce89bd70954697cf93d018e97eb80493&locations= | com/geoway/cloudquery/app/SurveyLogic.java |
| http://t6.tianditu.com/DataServer?T=img\_w&x= | com/geoway/cloudquery/app/MapHelper.java |
| http://t6.tianditu.com/DataServer?T=cia\_w&x= | com/geoway/cloudquery/app/MapHelper.java |
| http://t6.tianditu.com/DataServer?T=vec\_w&x= | com/geoway/cloudquery/app/MapHelper.java |
| http://t6.tianditu.com/DataServer?T=cva\_w&x= | com/geoway/cloudquery/app/MapHelper.java |
| http://t0.tianditu.com/DataServer?T=ter\_w&x= | com/geoway/cloudquery/app/MapHelper.java |
| https://webrd01.is.autonavi.com/appmaptile?lang=zh\_cn&size=1&scale=1&style=7&x= | com/geoway/cloudquery/app/MapHelper.java |
| http://192.168.253.25:6080/arcgis/rest/services/DZD/MapServer/tile/ | com/geoway/cloudquery/app/MapHelper.java |
| http://api.cellocation.com:81/wifi/?mac=%s&output=json\ | com/geoway/cloudquery/location/WifiLocUtil.java |
| http://%s:%s/uis/rest/transform/ts | com/geoway/cloudquery/location/WifiLocUtil.java |
| http://api.cellocation.com:81/cell/?mcc=%s&mnc=%s&lac=%s&ci=%s&output=json\ | com/geoway/cloudquery/location/WifiLocUtil.java |
| http://vip.cellocation.com/loc/1xl9vv83.php?cl=%s&wl=%s&output=json | com/geoway/cloudquery/location/WifiLocUtil.java |
| http://t6.tianditu.com/DataServer?T=img\_w&x= | com/geoway/cloudquery/camera/PicMapManager.java |
| http://t6.tianditu.com/DataServer?T=cia\_w&x= | com/geoway/cloudquery/camera/PicMapManager.java |
| http://t6.tianditu.com/DataServer?T=vec\_w&x= | com/geoway/cloudquery/camera/PicMapManager.java |
| http://t6.tianditu.com/DataServer?T=cva\_w&x= | com/geoway/cloudquery/camera/PicMapManager.java |
| https://console.tianditu.gov.cn/mapserver/vmap/tdt2018\_mercator/getMAP?x= | com/geoway/mobile/MainActivity.java |
| http://172.16.67.34:8066/ime-cloud/rest/World\_V20/terrain/data?level= | com/geoway/mobile/MainActivity.java |
| http://www.landcloud.org.cn:81/atlas-ime/rest/globe\_world\_terrain/terrain/data?level= | com/geoway/mobile/MainActivity.java |
| https://t1.tianditu.gov.cn/mapservice/swdx?x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=img\_w&x= | com/geoway/mobile/MainActivity.java |
| https://webst04.is.autonavi.com/appmaptile?style=6&x= | com/geoway/mobile/MainActivity.java |
| https://gss0.bdstatic.com/5bwHcj7lABFU8t\_jkk\_Z1zRvfdw6buu/it/u=x= | com/geoway/mobile/MainActivity.java |
| https://www.google.cn/maps/vt?lyrs=y&gl=cn&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=cia\_w&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=cva\_w&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.gov.cn/DataServer?T=vec\_w&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=img\_c&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=cia\_c&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=vec\_c&x= | com/geoway/mobile/MainActivity.java |
| http://t6.tianditu.com/DataServer?T=cva\_c&x= | com/geoway/mobile/MainActivity.java |
| http://ditu.zjzwfw.gov.cn/mapserver/data/zjvmapm/getData?x= | com/geoway/mobile/MainActivity.java |
| http://ditu.zjzwfw.gov.cn/fonts/ | com/geoway/mobile/MainActivity.java |
| https://maps.ynmap.cn/services/img/map/3857/2017/WMTS?SERVICE=WMTS&REQUEST=GetTile&VERSION=1.0.0&LAYER=tdtYnImg100cm2000\_2017&STYLE=default&TILEMATRIXSET=default&TILEMATRIX= | com/geoway/mobile/MainActivity.java |
| https://www.googleapis.com/geolocation/v1/geolocate?key=AIzaSyDLToSD04V2ylySZaswsUWZX9s-WCGDx5g | com/geoway/mobile/location/provider/AlxLocationManager.java |
| https://adiu.amap.com/ws/device/adius | com/loc/be.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/loc/cu.java |
| http://apilocate.amap.com/mobile/binary | com/loc/fi.java |
| http://dualstack-a.apilocate.amap.com/mobile/binary | com/loc/fi.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fi.java |
| https://restsdk.amap.com/sdk/compliance/params | com/loc/ao.java |
| http://restsdk.amap.com/sdk/compliance/params | com/loc/ao.java |
| http://restsdk.amap.com | com/loc/u.java |
| http://restsdk.amap.com/v3/place/text? | com/loc/a.java |
| http://restsdk.amap.com/v3/config/district? | com/loc/a.java |
| http://restsdk.amap.com/v3/place/around? | com/loc/a.java |
| https://restsdk.amap.com/v3/iasdkauth | com/loc/l.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/loc/l.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fn.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/fb.java |
| http://dualstack-arestapi.amap.com/v3/geocode/regeo | com/loc/fd.java |
| http://restsdk.amap.com/v3/geocode/regeo | com/loc/fd.java |
| http://www.chinapop.gov.cn/dataspec\ | com/nisc/SecurityEngine.java |
| https://(.\*)/por/perinfo.csp\\?pwp\_errorcode=(\\d+) | com/sangfor/ssl/vpn/common/aw.java |
| https://debugtbs.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugx5.qq.com | com/tencent/smtt/sdk/WebView.java |
| https://debugtbs.qq.com?10000\ | com/tencent/smtt/sdk/WebView.java |
| https://pms.mb.qq.com/rsp204 | com/tencent/smtt/sdk/m.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079 | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u= | com/tencent/smtt/sdk/stat/MttLoader.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041 | com/tencent/smtt/sdk/ui/dialog/d.java |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/n.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/n.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/n.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/n.java |
| https://tbsrecovery.imtt.qq.com/getconfig | com/tencent/smtt/utils/n.java |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/d.java |
| http://www.opengis.net/gml | com/vividsolutions/jts/io/gml2/GMLConstants.java |
| http://%s:%d | geoway/tdtlibrary/util/NetworkUtil.java |
| http://www.tianditu.com/mobile\_url/v223 | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://mobsv3.tianditu.com | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://mobile.tianditu.com/mobileversionandmessage/sendm.action | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://download.tianditu.com/download/mobile/layers201.xml | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://download.tianditu.com/download/mobile/download\_v23.xml | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://t6.tianditu.cn/DataServer? | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://download.tianditu.com/download/mobile/category.xml | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://mobile.tianditu.com/mobileversionandmessage/mobilev.action? | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://mobile.tianditu.com/mobileservice/bases.action | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://www.tianditu.com/query.shtml | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://mobile.tianditu.com/phoneService/route.do? | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://www.tianditu.cn/mobile\_url/weathercode | geoway/tdtlibrary/util/tdt/LoadServicesURL.java |
| http://www.tianditu.com/query.shtml?type=query&postStr= | geoway/tdtlibrary/search/support/PoiSearch.java |
| http://118.178.118.177/ime-server/rest/placesearch/place/search?format=json&page\_num=0&page\_size=10&q=%s&sq\_type=bounds&bounds=%f,%f,%f,%f | geoway/tdtlibrary/search/support/PoiSearch.java |
| http://www.andykhan.com/jexcelapi/index.html | jxl/read/biff/HyperlinkRecord.java |
| http://www.andykhan.com/jexcelapi/index.html | jxl/demo/ReadWrite.java |
| http://www.andykhan.com/jexcelapi | jxl/demo/Write.java |
| http://www.amazon.co.uk/exec/obidos/ASIN/0571058086/qid=1099836249/sr=1-3/ref=sr\_1\_11\_3/202-6017285-1620664 | jxl/demo/Write.java |
| http://www.andykhan.com/jexcelapi\ | jxl/demo/Write.java |
| http://www.amazon.co.uk/exec/obidos/ASIN/0571058086qid=1099836249/sr=1-3/ref=sr\_1\_11\_3/202-6017285-1620664\ | jxl/demo/Write.java |
| http://schemas.xmlsoap.org/soap/encoding/ | org/ksoap2/SoapEnvelope.java |
| http://schemas.xmlsoap.org/soap/envelope/ | org/ksoap2/SoapEnvelope.java |
| http://xml.apache.org/xml-soap | org/ksoap2/serialization/MarshalHashtable.java |
| http://www.wireless-village.org/CSP | org/kxml2/wap/wv/WV.java |
| http://www.wireless-village.org/PA | org/kxml2/wap/wv/WV.java |
| http://www.wireless-village.org/TRC | org/kxml2/wap/wv/WV.java |
| http://www.openmobilealliance.org/DTD/WV-CSP | org/kxml2/wap/wv/WV.java |
| http://www.openmobilealliance.org/DTD/WV-PA | org/kxml2/wap/wv/WV.java |
| http://www.openmobilealliance.org/DTD/WV-TRC | org/kxml2/wap/wv/WV.java |
| http://www. | org/kxml2/wap/wml/Wml.java |
| https://www. | org/kxml2/wap/wml/Wml.java |
| http://xmlpull.org/v1/doc/features.html | org/kxml2/io/KXmlSerializer.java |
| http://xmlpull.org/v1/doc/ | org/kxml2/io/KXmlParser.java |
| http://xmlpull.org/v1/doc/properties.html | org/kxml2/kdom/Document.java |
| http://xmlpull.org/v1/doc/features.html | org/xmlpull/v1/XmlPullParser.java |
| http://dev.dcloud.net.cn/mui) | 摸瓜V2引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| houfeng@dcloud.io | 摸瓜V2引擎 |
| houfeng@dcloud.io | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13305658818 | com/geoway/cloudquery/mgr/DisasterMgr.java |
| 15222222222 | com/loc/l.java |
| 13511111111 | com/nisc/Olym\_UnionSign\_SecurityEngine.java |
| 18222222222 | com/tencent/smtt/sdk/p.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: CN=emmkeystore, OU=ssl, O=sangfor, L=sz, ST=gd, C=cn 签名算法: rsassa\_pkcs1v15 有效期自: 2019-04-04 01:01:58+00:00 有效期至: 2039-03-30 01:01:58+00:00 发行人: CN=emmkeystore, OU=ssl, O=sangfor, L=sz, ST=gd, C=cn 序列号: 0x40903eb 哈希算法: sha256 md5值: af84165c19d9150b8b278e82135ad9cc sha1值: 44ccde4f7be1f4fdc3e2f5df97a10237a73d9552 sha256值: 225f96e888b1ff0d5a461cb0a4c2406f9a6f2ded207042e7d50b1a46a2c3c1fb sha512值: a0e7312845da5ec8b017f4b0a5bd08c3061b3ff787d11fdc0edfd2ee97010538cef4dc1b4becf5d3c6d77ff6b7f3b7aa9398d06a1afacfdd895241ab6e07f8b5 公钥算法: rsa 密钥长度: 1024 指纹: 3fff7d8e1d2b39fac5a40cfd34612e4bb155dea5141ea385eed26ac2c0a6ee22**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "nrtc\_setting\_other\_device\_default\_rotation\_key" : "nrtc\_setting\_other\_device\_default\_rotation\_key" |
| "nrtc\_setting\_other\_device\_rotation\_fixed\_offset\_key" : "nrtc\_setting\_other\_device\_rotation\_fixed\_offset\_key" |
| "nrtc\_setting\_other\_server\_record\_audio\_key" : "nrtc\_setting\_other\_server\_record\_audio\_key" |
| "nrtc\_setting\_other\_server\_record\_video\_key" : "nrtc\_setting\_other\_server\_record\_video\_key" |
| "nrtc\_setting\_vie\_crop\_key" : "nrtc\_setting\_vie\_crop\_key" |
| "nrtc\_setting\_vie\_default\_front\_camera\_key" : "nrtc\_setting\_vie\_default\_front\_camera\_key" |
| "nrtc\_setting\_vie\_fps\_reported\_key" : "nrtc\_setting\_vie\_fps\_reported\_key" |
| "nrtc\_setting\_vie\_hw\_decoder\_key" : "nrtc\_setting\_vie\_hw\_decoder\_key" |
| "nrtc\_setting\_vie\_hw\_encoder\_key" : "nrtc\_setting\_vie\_hw\_encoder\_key" |
| "nrtc\_setting\_vie\_max\_bitrate\_key" : "nrtc\_setting\_vie\_max\_bitrate\_key" |
| "nrtc\_setting\_vie\_muted\_key" : "nrtc\_setting\_vie\_muted\_key" |
| "nrtc\_setting\_vie\_quality\_key" : "nrtc\_setting\_vie\_quality\_key" |
| "nrtc\_setting\_vie\_rotation\_key" : "nrtc\_setting\_vie\_rotation\_key" |
| "nrtc\_setting\_voe\_audio\_aec\_key" : "nrtc\_setting\_voe\_audio\_aec\_key" |
| "nrtc\_setting\_voe\_audio\_ns\_key" : "nrtc\_setting\_voe\_audio\_ns\_key" |
| "nrtc\_setting\_voe\_call\_proximity\_key" : "nrtc\_setting\_voe\_call\_proximity\_key" |
| "nrtc\_setting\_voe\_dtx\_key" : "nrtc\_setting\_voe\_dtx\_key" |
| "nrtc\_setting\_voe\_high\_quality\_key" : "nrtc\_setting\_voe\_high\_quality\_key" |
| "nrtc\_setting\_voe\_muted\_key" : "nrtc\_setting\_voe\_muted\_key" |
| "record\_camera\_author" : "%1$s 作品" |

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_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.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.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.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 |
| com.fingerprints.service.ACCESS\_FINGERPRINT\_MANAGER | 未知 | Unknown permission | Unknown permission from android reference |
| com.samsung.android.providers.context.permission.WRITE\_USE\_APP\_FEATURE\_SURVEY | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| android.permission.ACCESS\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.UNINSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |

## **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。**