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

**广轻智慧校园3.0（ 1.3.33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 | 广轻智慧校园3.0 |
| 版本 | 1.3.33 |
| 包名 | com.zhycapp |
| 域名线索 | 58条 |
| URL线索 | 56条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | base.apk |
| 文件大小 | 183.96MB |
| MD5值 | 635c0afe08108ed7c38df646ae5ac944 |
| SHA1值 | 76b2fa5652fcbd94b14b1d941e0c184f09241ca4 |
| SHA256值 | e416a164b7ad02cec5c490e084eddc2b8426b1e5d1c02dc1ac69dd02933ea805 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 广轻智慧校园3.0 |
| 包名 | com.zhycapp |
| 主活动Activity | com.zhycapp.MainActivity |
| 安卓版本名称 | 1.3.33 |
| 安卓版本 | 101 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| play.google.com | IP: 59.24.3.174  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| relaxng.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.satip.info | IP: 35.214.201.169  所属国家: Netherlands  地区: Groningen  城市: Groningen |
| www.winimage.com | IP: 205.251.81.217  所属国家: United States of America  地区: New Jersey  城市: Parsippany |
| www.icecast.org | IP: 140.211.166.31  所属国家: United States of America  地区: Oregon  城市: Eugene |
| ns.adobe.com | 没有服务器地理信息. |
| lame.sf.net | IP: 104.18.20.237  所属国家: United States of America  地区: California  城市: San Francisco |
| www.tvdr.de | IP: 88.198.76.220  所属国家: Germany  地区: Bayern  城市: Gunzenhausen |
| lbs.amap.com | IP: 110.253.188.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| musicbrainz.org | IP: 142.132.240.1  所属国家: Germany  地区: Sachsen  城市: Falkenstein |
| fingerprint.videolan.org | IP: 213.36.253.2  所属国家: France  地区: Ile-de-France  城市: Paris |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.oasis-open.org | IP: 172.99.100.168  所属国家: United States of America  地区: Texas  城市: Windcrest |
| www.twolame.org | IP: 93.93.131.3  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Cambridge |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| www.facebook.com | IP: 185.60.216.50  所属国家: Ireland  地区: Dublin  城市: Dublin |
| mpsapi.amap.com | IP: 203.119.169.143  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| twitter.com | IP: 210.56.51.193  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.npes.org | IP: 104.21.43.185  所属国家: United States of America  地区: California  城市: San Francisco |
| lbs-3dtiles-service.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| ns.useplus.org | IP: 54.83.4.77  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| wprd0d.is.autonavi.com | 没有服务器地理信息. |
| dualstack-a.apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| ce3e75d5.jpush.cn | IP: 120.233.114.176  所属国家: China  地区: Guangdong  城市: Shenzhen |
| raw.githubusercontent.com | IP: 185.199.109.133  所属国家: United States of America  地区: Pennsylvania  城市: California |
| drewnoakes.com | IP: 34.229.76.186  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| wap.amap.com | IP: 116.142.235.231  所属国家: China  地区: Beijing  城市: Beijing |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| xerces.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| open.weixin.qq.com | IP: 140.207.191.167  所属国家: China  地区: Shanghai  城市: Shanghai |
| cipa.jp | IP: 118.82.81.189  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| restapi.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| plus.google.com | IP: 162.125.32.13  所属国家: United States of America  地区: California  城市: San Francisco |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| mps.amap.com | IP: 203.119.169.143  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| docs.swmansion.com | IP: 172.67.142.188  所属国家: United States of America  地区: California  城市: San Francisco |
| restsdk.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| maps.testing.amap.com | IP: 59.82.57.204  所属国家: China  地区: Beijing  城市: Beijing |
| www.webrtc.org | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| mst01.is.autonavi.com | IP: 110.253.189.212  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| www.videolan.org | IP: 213.36.253.2  所属国家: France  地区: Ile-de-France  城市: Paris |
| pinterest.com | IP: 192.133.77.133  所属国家: United States of America  地区: California  城市: San Francisco |
| long.open.weixin.qq.com | IP: 112.65.193.170  所属国家: China  地区: Shanghai  城市: Shanghai |
| iptc.org | IP: 3.64.29.21  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| ce3e75d5-ipv6.jpush.cn | IP: 120.233.33.225  所属国家: China  地区: Guangdong  城市: Shenzhen |
| m5.amap.com | IP: 59.82.112.99  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.ietf.org | IP: 104.16.45.99  所属国家: United States of America  地区: California  城市: San Francisco |
| www.aiim.org | IP: 199.60.103.225  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| pano.video | IP: 47.117.65.112  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cgicol.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| adiu.amap.com | IP: 110.253.188.148  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| www.shoutcast.coms | 没有服务器地理信息. |
| www.shoutcast.com | IP: 13.70.37.114  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| dualstack-arestapi.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| purl.org | IP: 207.241.225.157  所属国家: United States of America  地区: California  城市: San Francisco |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot | com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java |
| https://github.com/software-mansion/react-native-screens/issues/17 | com/swmansion/rnscreens/ScreenFragment.java |
| https://github.com/software-mansion/react-native-screens/issues/17 | com/swmansion/rnscreens/ScreenStackFragment.java |
| http://ns.adobe.com/StockPhoto/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/asf/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/bwf/bext/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/camera-raw-settings/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/creatorAtom/1.0/ | com/adobe/xmp/XMPConst.java |
| http://purl.org/dc/elements/1.1/ | com/adobe/xmp/XMPConst.java |
| http://purl.org/dc/1.1/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/DICOM/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/1.0/DynamicMedia/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/exif/1.0/ | com/adobe/xmp/XMPConst.java |
| http://cipa.jp/exif/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/exif/1.0/aux/ | com/adobe/xmp/XMPConst.java |
| http://iptc.org/std/Iptc4xmpCore/1.0/xmlns/ | com/adobe/xmp/XMPConst.java |
| http://iptc.org/std/Iptc4xmpExt/2008-02-29/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/iX/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/jp2k/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/jpeg/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/pdf/1.3/ | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/extension/ | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/field | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/id/ | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/property | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/schema | com/adobe/xmp/XMPConst.java |
| http://www.aiim.org/pdfa/ns/type | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/pdfx/1.3/ | com/adobe/xmp/XMPConst.java |
| http://www.npes.org/pdfx/ns/id/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/photoshop/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.useplus.org/ldf/xmp/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/png/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/album/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/riff/info/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/1.0/Script/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/swf/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/tiff/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/transient/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/TransformXMP/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/wav/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/bj/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/mm/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/note/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/rights/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/Dimensions | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/Font | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/g/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xmp/Identifier/qual/1.0/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/g/img/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/ManifestItem | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/t/pg/ | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/ResourceEvent | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/ResourceRef | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/Job | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/sType/Version | com/adobe/xmp/XMPConst.java |
| http://ns.adobe.com/xap/1.0/t/ | com/adobe/xmp/XMPConst.java |
| http://purl.org/dc/elements/1.1/ | com/adobe/xmp/impl/Utils.java |
| http://ns.adobe.com/xap/1.0/ | com/adobe/xmp/impl/Utils.java |
| http://ns.adobe.com/tiff/1.0/ | com/adobe/xmp/impl/Utils.java |
| http://ns.adobe.com/exif/1.0/ | com/adobe/xmp/impl/Utils.java |
| http://ns.adobe.com/exif/1.0/aux/ | com/adobe/xmp/impl/Utils.java |
| http://ns.adobe.com/xap/1.0/ | com/adobe/xmp/impl/XMPSerializerRDF.java |
| http://javax.xml.XMLConstants/feature/secure-processing | com/adobe/xmp/impl/XMPMetaParser.java |
| http://apache.org/xml/features/disallow-doctype-decl | com/adobe/xmp/impl/XMPMetaParser.java |
| http://xml.org/sax/features/external-general-entities | com/adobe/xmp/impl/XMPMetaParser.java |
| http://xerces.apache.org/xerces2-j/features.html | com/adobe/xmp/impl/XMPMetaParser.java |
| http://xml.org/sax/features/external-parameter-entities | com/adobe/xmp/impl/XMPMetaParser.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | com/adobe/xmp/impl/XMPMetaParser.java |
| http://ns.adobe.com/xap/1.0/ | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java |
| http://purl.org/dc/elements/1.1/ | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java |
| http://ns.adobe.com/tiff/1.0/ | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java |
| http://ns.adobe.com/exif/1.0/ | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java |
| http://ns.adobe.com/exif/1.0/aux/ | com/adobe/xmp/impl/XMPSchemaRegistryImpl.java |
| http://purl.org/dc/elements/1.1/ | com/adobe/xmp/impl/ParseRDF.java |
| http://purl.org/dc/elements/1.1/ | com/adobe/xmp/impl/XMPNormalizer.java |
| http://ns.adobe.com/exif/1.0/ | com/adobe/xmp/impl/XMPNormalizer.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://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/trans/a.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/autonavi/aps/amapapi/utils/g.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://m5.amap.com/ | com/autonavi/base/amap/mapcore/maploader/AMapLoader.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/data?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://wap.amap.com/ | com/amap/api/maps/AMapUtils.java |
| https://lbs-3dtiles-service.amap.com/basemap/tiles/staging?compose=building@1669011850923&compose=tree@1668678765481&z=%d&x=%d&y=%d | com/amap/api/maps/model/amap3dmodeltile/AMap3DModelTileProvider.java |
| http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/\ | com/amap/api/col/p0003l/l.java |
| https://restsdk.amap.com/v3/iasdkauth | com/amap/api/col/p0003l/fh.java |
| https://dualstack-arestapi.amap.com/v3/iasdkauth | com/amap/api/col/p0003l/fh.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003l/s.java |
| http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74& | com/amap/api/col/p0003l/jm.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003l/df.java |
| http://restsdk.amap.com/v3/place/text? | com/amap/api/col/p0003l/a.java |
| http://restsdk.amap.com/v3/place/around? | com/amap/api/col/p0003l/a.java |
| http://restsdk.amap.com/v3/config/district? | com/amap/api/col/p0003l/a.java |
| http://restsdk.amap.com | com/amap/api/col/p0003l/v.java |
| https://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003l/hc.java |
| http://restsdk.amap.com/sdk/compliance/params | com/amap/api/col/p0003l/hc.java |
| https://adiu.amap.com/ws/device/adius | com/amap/api/col/p0003l/hs.java |
| http://restsdk.amap.com/v4/grasproad/driving? | com/amap/api/col/p0003l/fb.java |
| http://restsdk.amap.com/v4 | com/amap/api/col/p0003l/cr.java |
| http://wprd0%d.is.autonavi.com/appmaptile? | com/amap/api/col/p0003l/de.java |
| http://restsdk.amap.com/v4/gridmap? | com/amap/api/col/p0003l/de.java |
| http://restsdk.amap.com | com/amap/api/col/p0003l/fq.java |
| https://restapi.amap.com/rest/aaid/get | com/amap/api/col/p0003l/ga.java |
| http://restapi.amap.com/rest/aaid/get | com/amap/api/col/p0003l/ga.java |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java |
| https://drewnoakes.com/code/exif/\n | com/drew/tools/ProcessAllImagesInFolderUtility.java |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/%s) | com/drew/tools/ProcessAllImagesInFolderUtility.java |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s/metadata/%s.txt)\n | com/drew/tools/ProcessAllImagesInFolderUtility.java |
| http://purl.org/dc/elements/1.1/ | com/drew/metadata/Schema.java |
| http://ns.adobe.com/exif/1.0/aux/ | com/drew/metadata/Schema.java |
| http://ns.adobe.com/exif/1.0/ | com/drew/metadata/Schema.java |
| http://ns.adobe.com/tiff/1.0/ | com/drew/metadata/Schema.java |
| http://ns.adobe.com/xap/1.0/ | com/drew/metadata/Schema.java |
| http://ns.adobe.com/xmp/note/ | com/drew/metadata/xmp/XmpReader.java |
| http://ns.adobe.com/xmp/extension/\u0000 | com/drew/metadata/xmp/XmpReader.java |
| http://ns.adobe.com/xap/1.0/\u0000 | com/drew/metadata/xmp/XmpReader.java |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s\ | com/drew/imaging/ImageMetadataReader.java |
| https://ce3e75d5.jpush.cn/wi/cjc4sa | cn/jiguang/bf/c.java |
| https://ce3e75d5-ipv6.jpush.cn/wi/cjc4sa | cn/jiguang/bf/c.java |
| https://ce3e75d5.jpush.cn/wi/d8n3hj | cn/jiguang/bf/c.java |
| https://ce3e75d5-ipv6.jpush.cn/wi/d8n3hj | cn/jiguang/bf/c.java |
| https://play.google.com/store/apps/details?id=com.instagram.android | cl/json/social/InstagramStoriesShare.java |
| https://pinterest.com/pin/create/button/?url= | cl/json/social/PinterestShare.java |
| https://plus.google.com/share?url= | cl/json/social/GooglePlusShare.java |
| https://www.facebook.com/sharer/sharer.php?u= | cl/json/social/FacebookShare.java |
| https://twitter.com/intent/tweet?text= | cl/json/social/TwitterShare.java |
| https://www.facebook.com/sharer/sharer.php?u= | cl/json/social/FacebookPagesManagerShare.java |
| https://play.google.com/store/apps/details?id=com.instagram.android | cl/json/social/InstagramShare.java |
| http://%s%s%s | lib/armeabi-v7a/libvlc.so |
| http://www.shoutcast.com/sbin/newxml.phtml?genre=%s | lib/armeabi-v7a/libvlc.so |
| http://www.shoutcast.com/sbin/tunein-tvstation.pls?id=%s | lib/armeabi-v7a/libvlc.so |
| http://www.shoutcast.com%s?id=%s | lib/armeabi-v7a/libvlc.so |
| http://www.videolan.org/vlc/playlist/0 | lib/armeabi-v7a/libvlc.so |
| http://musicbrainz.org | lib/armeabi-v7a/libvlc.so |
| http://www.satip.info/Playlists/%s.m3u | lib/armeabi-v7a/libvlc.so |
| http://location | lib/armeabi-v7a/libvlc.so |
| http://%s:%d | lib/armeabi-v7a/libvlc.so |
| http://%s%s | lib/armeabi-v7a/libvlc.so |
| http://%s:%d%s | lib/armeabi-v7a/libvlc.so |
| http://%s:8008%s | lib/armeabi-v7a/libvlc.so |
| http://www.tvdr.de/). | lib/armeabi-v7a/libvlc.so |
| https://fingerprint.videolan.org/acoustid.php?meta=recordings+tracks+usermeta+releases&duration=%d&fingerprint=%s | lib/armeabi-v7a/libvlc.so |
| http://www.videolan.org/vlc | lib/armeabi-v7a/libvlc.so |
| http://lame.sf.net | lib/armeabi-v7a/libvlc.so |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd | lib/armeabi-v7a/libvlc.so |
| http://relaxng.org/ns/structure/1.0 | lib/armeabi-v7a/libvlc.so |
| http://[ | lib/armeabi-v7a/libvlc.so |
| http://www.icecast.org/ | lib/armeabi-v7a/libvlc.so |
| http://www.twolame.org/ | lib/armeabi-v7a/libvlc.so |
| http://www.videolan.org/x264.html | lib/armeabi-v7a/libvlc.so |
| http://ns.adobe.com/xap/1.0/ | lib/armeabi-v7a/libvlc.so |
| http://http | lib/armeabi-v7a/libbarhopper\_v2.so |
| http://ns.adobe.com/xap/1.0/ | lib/armeabi-v7a/libnative-imagetranscoder.so |
| http://mpsapi.amap.com/ws/mps/vmap/ | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/rtt/ | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/smap | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://m5.amap.com | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/rtt | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/vmap | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/smap | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/spot | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/hot | lib/armeabi-v7a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://www.winimage.com/zLibDll | lib/armeabi-v7a/libpanortc.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/armeabi-v7a/libpanortc.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/armeabi-v7a/libpanortc.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/armeabi-v7a/libpanortc.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/armeabi-v7a/libpanortc.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/armeabi-v7a/libpanortc.so |
| http://pano.video/html/framemarking | lib/armeabi-v7a/libpanortc.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/armeabi-v7a/libpanortc.so |
| http://%s%s%s | lib/arm64-v8a/libvlc.so |
| http://www.tvdr.de/). | lib/arm64-v8a/libvlc.so |
| http://www.satip.info/Playlists/%s.m3u | lib/arm64-v8a/libvlc.so |
| http://ns.adobe.com/xap/1.0/ | lib/arm64-v8a/libvlc.so |
| http://%s:%d | lib/arm64-v8a/libvlc.so |
| http://www.videolan.org/vlc | lib/arm64-v8a/libvlc.so |
| http://%s%s | lib/arm64-v8a/libvlc.so |
| http://%s:%d%s | lib/arm64-v8a/libvlc.so |
| https://fingerprint.videolan.org/acoustid.php?meta=recordings+tracks+usermeta+releases&duration=%d&fingerprint=%s | lib/arm64-v8a/libvlc.so |
| http://location | lib/arm64-v8a/libvlc.so |
| http://musicbrainz.org | lib/arm64-v8a/libvlc.so |
| http://www.shoutcast.com/sbin/newxml.phtml?genre=%s | lib/arm64-v8a/libvlc.so |
| http://www.shoutcast.com/sbin/tunein-tvstation.pls?id=%s | lib/arm64-v8a/libvlc.so |
| http://www.shoutcast.com%s?id=%s | lib/arm64-v8a/libvlc.so |
| http://www.videolan.org/vlc/playlist/0 | lib/arm64-v8a/libvlc.so |
| http://%s:8008%s | lib/arm64-v8a/libvlc.so |
| http://lame.sf.net | lib/arm64-v8a/libvlc.so |
| http://www.oasis-open.org/committees/entity/release/1.0/catalog.dtd | lib/arm64-v8a/libvlc.so |
| http://relaxng.org/ns/structure/1.0 | lib/arm64-v8a/libvlc.so |
| http://[ | lib/arm64-v8a/libvlc.so |
| http://www.icecast.org/ | lib/arm64-v8a/libvlc.so |
| http://www.twolame.org/ | lib/arm64-v8a/libvlc.so |
| http://www.videolan.org/x264.html | lib/arm64-v8a/libvlc.so |
| http://http | lib/arm64-v8a/libbarhopper\_v2.so |
| http://mpsapi.amap.com/ws/mps/vmap/ | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/rtt/ | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/smap | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://m5.amap.com/ws/transfer/auth/map/indoor\_maps | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ws/mps/lyrdata/ugc/ | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://mpsapi.amap.com/ | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| http://m5.amap.com | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/rtt | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/vmap | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://maps.testing.amap.com/ws/transfer/auth/map/indoor\_maps | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/smap | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/spot | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |
| https://mps.amap.com/ws/mps/hot | lib/arm64-v8a/libAMapSDK\_MAP\_v9\_6\_0.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| sam@zoy.org  libdvbpsi-devel@videolan.org  fsync@openssh.com  fstatvfs@openssh.com  statvfs@openssh.com  a2-nistp256-cert-v01@openssh.com  a2-nistp384-cert-v01@openssh.com  a2-nistp521-cert-v01@openssh.com  auth-agent-req@openssh.com  rijndael-cbc@lysator.liu  hmac-ripemd160@openssh.com  zlib@openssh.com  twolame-discuss@lists.sourceforg  keepalive@libssh2.orgw | lib/armeabi-v7a/libvlc.so |
| android-sdk-releaser@ljlg19.prod | lib/armeabi-v7a/libbarhopper\_v2.so |
| sam@zoy.org  libdvbpsi-devel@videolan.org  fsync@openssh.com  fstatvfs@openssh.com  a2-nistp256-cert-v01@openssh.com  a2-nistp384-cert-v01@openssh.com  a2-nistp521-cert-v01@openssh.com  keepalive@libssh2.orgw  auth-agent-req@openssh.com  rijndael-cbc@lysator.liu  hmac-ripemd160@openssh.com  zlib@openssh.com  twolame-discuss@lists.sourceforg | lib/arm64-v8a/libvlc.so |
| android-sdk-releaser@ljlg19.prod | lib/arm64-v8a/libbarhopper\_v2.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15222222222 | com/amap/api/col/p0003l/fh.java |
| 14389071831 | lib/armeabi-v7a/libvlc.so |
| 14389071831 | lib/arm64-v8a/libvlc.so |

## **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=china, ST=guangdong, L=guangzhou, O=zhyc, OU=zhyc, CN=zhong 签名算法: rsassa\_pkcs1v15 有效期自: 2019-07-26 10:14:46+00:00 有效期至: 2046-12-11 10:14:46+00:00 发行人: C=china, ST=guangdong, L=guangzhou, O=zhyc, OU=zhyc, CN=zhong 序列号: 0x6c975d34 哈希算法: sha256 md5值: 959008c1d408aae29150a74add51f9c5 sha1值: 3570d4af9135e293af4e1108a10aca566c57d155 sha256值: 0eb5a9f5de7427fa0be785e6c0923c86c8657971724ff71e3448cebbdc00fdee sha512值: c11f16258d8aae8495f018ca7835a090028744135130c3401c46fad197a716b00da7e71c044dd6c0b0a3050a9cefa8156ad43347ba3d22e0ffd4e0e5f0d345c8 公钥算法: rsa 密钥长度: 2048 指纹: e0f6f70c5be4b18fd04dd889bbe476724a4d042d4c219e2cfe8292fe6cfa053e**

## **6. 硬编码敏感信息**

## **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 |
| --- | --- | --- | --- |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.hihonor.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| 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.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。 |
| com.zhycapp.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| android.permission.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。 |
| com.android.vending.CHECK\_LICENSE | 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 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |

## **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。**