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

**普适排口（ 4.1.8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 | 普适排口 |
| 版本 | 4.1.8 |
| 包名 | com.pushi |
| 域名线索 | 56条 |
| URL线索 | 38条 |
| APP图标 |  |
| 分析日期 | 2024年10月18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 | pspk.apk |
| 文件大小 | 40.98MB |
| MD5值 | db69ab7e8daaf14cc1ce869cb6a077c6 |
| SHA1值 | 40d0c0003eb7c714547eb1784a5ed0e06425db13 |
| SHA256值 | 0c7b58c72beacc2c41c7a3104953231f34bc3bd3c5788f94e43c4dfcb74ac6f4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 普适排口 |
| 包名 | com.pushi |
| 主活动Activity | com.pushi.MainActivity |
| 安卓版本名称 | 4.1.8 |
| 安卓版本 | 418 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ns.useplus.org | IP: 54.83.4.77  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| xml.org | IP: 104.239.240.11  所属国家: United States of America  地区: Texas  城市: Windcrest |
| dualstack.apilocate.amap.com | IP: 106.11.40.50  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| oss-cn-hangzhou.aliyuncs.com | IP: 118.31.219.250  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| image.cnamedomain.com | 没有服务器地理信息. |
| oss-cn-.aliyuncs.comor | 没有服务器地理信息. |
| maps.google.com | IP: 142.251.43.14  所属国家: United States of America  地区: California  城市: Mountain View |
| docs.swmansion.com | IP: 172.67.142.188  所属国家: United States of America  地区: California  城市: San Francisco |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| paulbourke.net | IP: 216.137.177.54  所属国家: United States of America  地区: Michigan  城市: Ann Arbor |
| 139.224.72.67 | IP: 139.224.72.67  所属国家: China  地区: Shanghai  城市: Shanghai |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.google.com | IP: 199.59.148.20  所属国家: United States of America  地区: California  城市: San Francisco |
| apilocate.amap.com | IP: 106.11.43.81  所属国家: China  地区: Beijing  城市: Beijing |
| earth.google.com | IP: 172.217.163.46  所属国家: United States of America  地区: California  城市: Mountain View |
| oss.aliyuncs.com | IP: 118.178.29.5  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| drewnoakes.com | IP: 34.229.76.186  所属国家: United States of America  地区: Virginia  城市: Ashburn |
| www.opengis.net | IP: 66.244.86.70  所属国家: United States of America  地区: Indiana  城市: Bloomington |
| xerces.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| raw.githubusercontent.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| schemas.opengis.net | IP: 66.244.86.52  所属国家: United States of America  地区: Indiana  城市: Bloomington |
| cipa.jp | IP: 118.82.81.189  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.aiim.org | IP: 199.60.103.225  所属国家: United States of America  地区: Massachusetts  城市: Cambridge |
| adiu.amap.com | IP: 203.119.204.133  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.topografix.com | IP: 104.209.197.87  所属国家: United States of America  地区: Virginia  城市: Boydton |
| 221.181.88.134 | IP: 221.181.88.134  所属国家: China  地区: Shanghai  城市: Shanghai |
| developers.google.com | IP: 142.251.42.238  所属国家: United States of America  地区: California  城市: Mountain View |
| stamen.com | IP: 141.193.213.10  所属国家: United States of America  地区: Texas  城市: Austin |
| ns.adobe.com | 没有服务器地理信息. |
| ubinavi-paikou.oss-cn-shanghai.aliyuncs.com | IP: 47.101.83.173  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| lbs.amap.com | IP: 110.253.189.211  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| perfectionkills.com | IP: 192.30.252.153  所属国家: United States of America  地区: California  城市: San Francisco |
| codepush.appcenter.ms | IP: 52.232.227.249  所属国家: United States of America  地区: Virginia  城市: Boydton |
| mobile.events.data.microsoft.com | IP: 20.189.173.5  所属国家: United States of America  地区: California  城市: San Francisco |
| aps.testing.amap.com | IP: 140.205.69.9  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.npes.org | IP: 104.21.43.185  所属国家: United States of America  地区: California  城市: San Francisco |
| dualstack-restapi.amap.com | IP: 39.98.22.142  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| pushi.ubinavi.com.cn | IP: 221.181.88.134  所属国家: China  地区: Shanghai  城市: Shanghai |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| www.microsoft.com | IP: 218.58.101.49  所属国家: China  地区: Shandong  城市: Zibo |
| abroad.apilocate.amap.com | IP: 59.82.44.11  所属国家: China  地区: Shanghai  城市: Shanghai |
| dev.dcloud.net.cn | IP: 116.136.188.184  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| 192.168.2.45 | IP: 192.168.2.45  所属国家: -  地区: -  城市: - |
| ask.dcloud.net.cn | IP: 119.188.180.230  所属国家: China  地区: Shandong  城市: Jinan |
| in.appcenter.ms | IP: 52.247.72.241  所属国家: United States of America  地区: Virginia  城市: Boydton |
| dev.virtualearth.net | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| openlayers.org | IP: 104.21.51.32  所属国家: United States of America  地区: California  城市: San Francisco |
| mapserver.gis.umn.edu | IP: 140.211.15.3  所属国家: United States of America  地区: Oregon  城市: Eugene |
| creativecommons.org | IP: 172.67.1.191  所属国家: United States of America  地区: California  城市: San Francisco |
| restapi.amap.com | IP: 59.82.132.217  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| iptc.org | IP: 3.64.29.21  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.openstreetmap.org | IP: 185.45.6.57  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: London |
| 127.0.0.1 | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.movable-type.co.uk | IP: 88.98.24.69  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Rochdale |
| purl.org | IP: 207.241.239.241  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 |
| --- | --- |
| 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/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://ns.adobe.com/xap/1.0/ | com/adobe/xmp/impl/XMPSerializerRDF.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://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 |
| https://ip. | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/OSSImpl.java |
| http://oss-cn-hangzhou.aliyuncs.com | com/alibaba/sdk/android/oss/common/OSSConstants.java |
| http://oss.aliyuncs.com | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://127.0.0.1 | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://oss-cn-\*\*\*\*.aliyuncs.com',or | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| http://image.cnamedomain.com'! | com/alibaba/sdk/android/oss/internal/InternalRequestOperation.java |
| https://raw.githubusercontent.com/drewnoakes/metadata-extractor-images/master/%s\ | com/drew/imaging/ImageMetadataReader.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://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://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/ | com/amap/api/location/AMapLocation.java |
| https://adiu.amap.com/ws/device/adius | com/loc/av.java |
| http://apilocate.amap.com/mobile/binary | com/loc/en.java |
| http://dualstack.apilocate.amap.com/mobile/binary | com/loc/en.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/en.java |
| http://aps.testing.amap.com/collection/collectData?src=baseCol&ver=v74& | com/loc/cf.java |
| http://restapi.amap.com | com/loc/s.java |
| http://restapi.amap.com/v3/place/text? | com/loc/a.java |
| http://restapi.amap.com/v3/config/district? | com/loc/a.java |
| http://restapi.amap.com/v3/place/around? | com/loc/a.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/er.java |
| http://abroad.apilocate.amap.com/mobile/binary | com/loc/eg.java |
| http://dualstack-restapi.amap.com/v3/geocode/regeo | com/loc/ei.java |
| http://restapi.amap.com/v3/geocode/regeo | com/loc/ei.java |
| https://restapi.amap.com/v3/iasdkauth | com/loc/l.java |
| http://restapi.amap.com/v3/iasdkauth | com/loc/l.java |
| https://in.appcenter.ms | com/microsoft/appcenter/ingestion/AppCenterIngestion.java |
| https://mobile.events.data.microsoft.com/OneCollector/1.0 | com/microsoft/appcenter/ingestion/OneCollectorIngestion.java |
| https://codepush.appcenter.ms/ | com/microsoft/codepush/react/CodePush.java |
| http://139.224.72.67:8081/outletcloud/ | com/pushi/BuildConfig.java |
| http://pushi.ubinavi.com.cn:8081/imgeditor/ | com/pushi/BuildConfig.java |
| https://ubinavi-paikou.oss-cn-shanghai.aliyuncs.com/outletImgList/ | com/pushi/BuildConfig.java |
| http://221.181.88.134:8081/ubireportapi/burying-point-record/report | com/pushi/BuildConfig.java |
| 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/ScreenStackFragment.java |
| https://github.com/software-mansion/react-native-screens/issues/17 | com/swmansion/rnscreens/ScreenFragment.java |
| http://139.224.72.67:8081/outletcloud/ | 摸瓜V1引擎 |
| http://pushi.ubinavi.com.cn:8081/imgeditor/ | 摸瓜V1引擎 |
| https://ubinavi-paikou.oss-cn-shanghai.aliyuncs.com/outletImgList/ | 摸瓜V1引擎 |
| http://221.181.88.134:8081/ubireportapi/burying-point-record/report | 摸瓜V1引擎 |
| http://t | 摸瓜V2引擎 |
| http://192.168.2.45:6080/arcgis/rest/services/pudong202207/MapServer/tile/ | 摸瓜V2引擎 |
| http://pushi.ubinavi.com.cn:26688/geoserver/pushi/wms?service=WMS' | 摸瓜V2引擎 |
| https://restapi.amap.com/v3/assistant/coordinate/convert?coordsys=gps&key=8aa60321bc4665ecd66aea2854cf82ef&locations=' | 摸瓜V2引擎 |
| https://restapi.amap.com/v3/geocode/regeo?key=8aa60321bc4665ecd66aea2854cf82ef&location=' | 摸瓜V2引擎 |
| https://openlayers.org/en/ | 摸瓜V2引擎 |
| http://www.movable-type.co.uk/scripts/latlong.html | 摸瓜V2引擎 |
| http://www.opengis.net/gml/srs/epsg.xml | 摸瓜V2引擎 |
| http://paulbourke.net/geometry/pointlineplane/).\n | 摸瓜V2引擎 |
| https://dev.virtualearth.net/REST/v1/Imagery/Metadata/ | 摸瓜V2引擎 |
| https://www.microsoft.com/maps/product/terms.html | 摸瓜V2引擎 |
| https://www.openstreetmap.org/copyright | 摸瓜V2引擎 |
| https://stamen.com/ | 摸瓜V2引擎 |
| https://creativecommons.org/licenses/by/3.0/ | 摸瓜V2引擎 |
| https://stamen-tiles- | 摸瓜V2引擎 |
| http://www.opengis.net/gml | 摸瓜V2引擎 |
| http://schemas.opengis.net/gml/3.1.1/profiles/gmlsfProfile/1.0.0/gmlsf.xsd | 摸瓜V2引擎 |
| http://schemas.opengis.net/gml/2.1.2/feature.xsd | 摸瓜V2引擎 |
| http://schemas.opengis.net/gml/3.2.1/gml.xsd | 摸瓜V2引擎 |
| http://www.opengis.net/gml/3.2 | 摸瓜V2引擎 |
| http://www.topografix.com/GPX/1/0 | 摸瓜V2引擎 |
| http://www.topografix.com/GPX/1/1 | 摸瓜V2引擎 |
| http://www.topografix.com/GPX/1/1/gpx.xsd | 摸瓜V2引擎 |
| http://www.google.com/kml/ext/2.2 | 摸瓜V2引擎 |
| http://earth.google.com/kml/2.0 | 摸瓜V2引擎 |
| http://earth.google.com/kml/2.1 | 摸瓜V2引擎 |
| http://earth.google.com/kml/2.2 | 摸瓜V2引擎 |
| http://www.opengis.net/kml/2.2 | 摸瓜V2引擎 |
| https://maps.google.com/mapfiles/kml/pushpin/ylw-pushpin.png | 摸瓜V2引擎 |
| https://developers.google.com/kml/schema/kml22gx.xsd | 摸瓜V2引擎 |
| http://www.opengis.net/wfs | 摸瓜V2引擎 |
| http://www.opengis.net/ogc | 摸瓜V2引擎 |
| http://www.opengis.net/fes | 摸瓜V2引擎 |
| http://schemas.opengis.net/wfs/1.1.0/wfs.xsd | 摸瓜V2引擎 |
| http://schemas.opengis.net/wfs/1.0.0/wfs.xsd | 摸瓜V2引擎 |
| http://www.opengis.net/wms | 摸瓜V2引擎 |
| http://mapserver.gis.umn.edu/mapserver | 摸瓜V2引擎 |
| http://www.opengis.net/ows/1.1 | 摸瓜V2引擎 |
| http://www.opengis.net/wmts/1.0 | 摸瓜V2引擎 |
| http://dev.dcloud.net.cn/mui) | 摸瓜V2引擎 |
| http://ask.dcloud.net.cn/article/113'; | 摸瓜V2引擎 |
| http://perfectionkills.com/global-eval-what-are-the-options/ | 摸瓜V2引擎 |
| http://ns.adobe.com/xap/1.0/ | lib/armeabi-v7a/libnative-imagetranscoder.so |

### **4.3 邮箱线索**

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

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15569251296 | net/time4j/calendar/VietnameseCalendar.java |
| 15569251296 | net/time4j/calendar/KoreanCalendar.java |
| 15569251296 | net/time4j/calendar/ChineseCalendar.java |
| 14403429586 | net/time4j/calendar/hindu/HinduVariant.java |
| 15040511099 | net/time4j/tz/model/SPX.java |
| 18067104000 | net/time4j/tz/model/SPX.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=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 签名算法: rsassa\_pkcs1v15 有效期自: 2013-12-31 22:35:04+00:00 有效期至: 2052-04-30 22:35:04+00:00 发行人: C=US, ST=Unknown, L=Unknown, O=Unknown, OU=Android, CN=Android Debug 序列号: 0x232eae62 哈希算法: sha1 md5值: 20f46148b72d8e5e5ca23d37a4f41490 sha1值: 5e8f16062ea3cd2c4a0d547876baa6f38cabf625 sha256值: fac61745dc0903786fb9ede62a962b399f7348f0bb6f899b8332667591033b9c sha512值: 926c0550edaee7aed1211b91fde06be4cc4748e61d8f1afbe0bd12f3949a0d09a1cf4306c72e6662ae4c7b8ae7a573a81d7e52e5b6124444eaf8f413e6b1fa69 公钥算法: rsa 密钥长度: 2048 指纹: b759a55bdc298b16f7a102f3107f3db38110f3dc7da00b1e981e9b257a9cf1af**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CodePushDeploymentKey" : "PP-n3yVidI5D9cpqTmHe7lh3UxLlJ-\_BbvKez" |

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.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.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. DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| android.permission.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.ACCESS\_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.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.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.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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。**