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

**OKPAY（ 2.0.0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 | OKPAY |
| 版本 | 2.0.0 |
| 包名 | com.oneworld.onepay |
| 域名线索 | 67条 |
| URL线索 | 50条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | com.oneworld.onepay\_c7fd5e1d.apk |
| 文件大小 | 16.41MB |
| MD5值 | b60a3ccce764f3d1683a1c9fd1490525 |
| SHA1值 | e91f8277121194264b21678894031b8a7877f3ce |
| SHA256值 | 75242162482280c28f68b9af5c58ebb59d966fac8a22f4489cd23fa98d1d54f6 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | OKPAY |
| 包名 | com.oneworld.onepay |
| 主活动Activity | com.leo.okp.MainActivity |
| 安卓版本名称 | 2.0.0 |
| 安卓版本 | 200 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.google-analytics.com | IP: 58.254.149.161 所属国家: China 地区: Guangdong 城市: Yunfu  |
| www.jivesoftware.com | IP: 23.235.209.143 所属国家: United States of America 地区: Virginia 城市: Virginia Beach  |
| norma-external-collect.meizu.com | IP: 122.13.76.176 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| dashif.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| store-drru.hispace.hicloud.com | IP: 159.138.202.186 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| plbslog.umeng.com | IP: 36.156.202.78 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| oss20231101.okfy8899.com | IP: 172.66.43.44 所属国家: United States of America 地区: California 城市: San Francisco  |
| idmb.register.xmpush.global.xiaomi.com | IP: 13.233.242.220 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| pagead2.googlesyndication.com | IP: 58.254.137.166 所属国家: China 地区: Guangdong 城市: Yunfu  |
| store3.hispace.hicloud.com | IP: 23.55.129.49 所属国家: Australia 地区: New South Wales 城市: Sydney  |
| alogsus.umeng.com | IP: 223.109.148.179 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| xml.org | IP: 104.239.240.11 所属国家: United States of America 地区: Texas 城市: Windcrest  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.apple.com | IP: 17.253.87.206 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| developer.android.com | IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View  |
| ulogs.umeng.com | IP: 223.109.148.130 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| www.jsdelivr.com | IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| store-at-dre.hispace.dbankcloud.com | 没有服务器地理信息.  |
| resolver.msg.global.xiaomi.net | IP: 47.241.174.254 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| store1.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| fr.register.xmpush.global.xiaomi.com | IP: 35.157.188.46 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| ssl.google-analytics.com | IP: 58.254.149.233 所属国家: China 地区: Guangdong 城市: Yunfu  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| developer.mozilla.org | IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City  |
| cn.register.xmpush.xiaomi.com | IP: 111.202.1.240 所属国家: China 地区: Beijing 城市: Beijing  |
| www.ibm.com | IP: 23.13.189.250 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.okpay777.com | IP: 35.220.164.170 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| aomedia.org | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ru.register.xmpush.global.xiaomi.com | IP: 107.155.52.56 所属国家: Russian Federation 地区: Moskva 城市: Moscow  |
| api.flutter.dev | IP: 199.36.158.100 所属国家: United States of America 地区: California 城市: Mountain View  |
| schemas.microsoft.com | IP: 13.107.246.74 所属国家: United States of America 地区: Washington 城市: Redmond  |
| api-push.in.meizu.com | IP: 206.161.233.191 所属国家: United States of America 地区: Virginia 城市: Herndon  |
| adash.man.aliyuncs.com | IP: 59.82.40.77 所属国家: China 地区: Shanghai 城市: Shanghai  |
| alogus.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| register.xmpush.global.xiaomi.com | IP: 47.88.199.5 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| storage.googleapis.com | IP: 142.251.42.251 所属国家: United States of America 地区: California 城市: Mountain View  |
| pslog.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| resolver.msg.xiaomi.net | IP: 123.125.102.48 所属国家: China 地区: Beijing 城市: Beijing  |
| plus.google.com | IP: 157.240.16.50 所属国家: India 地区: Maharashtra 城市: Mumbai  |
| store2.hispace.hicloud.com | IP: 13.225.183.110 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| ok1112817899.oss-cn-hangzhou.aliyuncs.com | IP: 118.178.29.145 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| api-push.meizu.com | IP: 221.5.93.66 所属国家: China 地区: Guangdong 城市: Foshan  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| xmlpull.org | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| grs.dbankcloud.com | IP: 113.201.107.54 所属国家: China 地区: Shaanxi 城市: Baoji  |
| developer.umeng.com | IP: 59.82.112.112 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| okzuixin1118899.oss-cn-beijing.aliyuncs.com | IP: 59.110.190.158 所属国家: China 地区: Beijing 城市: Beijing  |
| exoplayer.dev | IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics1.data.hicloud.com | IP: 218.12.91.83 所属国家: China 地区: Hebei 城市: Baoding  |
| play.google.com | IP: 59.24.3.174 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Seongnam  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| aaid.umeng.com | IP: 112.85.139.75 所属国家: China 地区: Jiangsu 城市: Nantong  |
| store.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| goo.gl | IP: 142.251.42.238 所属国家: United States of America 地区: California 城市: Mountain View  |
| grs.dbankcloud.asia | IP: 119.8.176.197 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| ns.adobe.com | 没有服务器地理信息.  |
| ouplog.umeng.com | IP: 47.246.110.93 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://adash.man.aliyuncs.com/man/api?ak=23356390&s=  | com/alibaba/sdk/android/utils/AMSDevReporter.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/DocumentBuilderFactorySecurity.java  |
| http://xml.org/sax/features/namespaces  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/namespace-prefixes  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/validation  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-general-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/external-parameter-entities  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xml.org/sax/features/string-interning  | com/huawei/secure/android/common/xml/SAXParserFactorySecurity.java  |
| http://xmlpull.org/v1/doc/features.html  | com/huawei/secure/android/common/xml/XmlPullParserFactorySecurity.java  |
| https://api-push.meizu.com/garcia/api/server/getPublicKey  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.in.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/android/exchange/getpublickey.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://norma-external-collect.meizu.com/push/android/external/add.do  | com/meizu/cloud/pushsdk/constants/PushConstants.java  |
| https://api-push.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.in.meizu.com/garcia/api/client/  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| https://api-push.meizu.com/garcia/api/client/log/upload  | com/meizu/cloud/pushsdk/platform/a/a.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| https://developer.umeng.com/docs/119267/detail/182050  | com/umeng/commonsdk/debug/UMLogCommon.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://%1$s/gslb/?ver=4.0  | com/xiaomi/push/cu.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gp.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/gd.java  |
| http://www.jivesoftware.com/xmlns/xmpp/properties\  | com/xiaomi/push/ha.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/hh.java  |
| http://xmlpull.org/v1/doc/features.html  | com/xiaomi/push/hi.java  |
| https://resolver.msg.global.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| https://resolver.msg.xiaomi.net/psc/?t=a  | com/xiaomi/push/service/bt.java  |
| https://cn.register.xmpush.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://fr.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://ru.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| https://idmb.register.xmpush.global.xiaomi.com  | com/xiaomi/push/service/s.java  |
| http://ns.adobe.com/xap/1.0/\u0000  | i/e/a/a.java  |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/PlatformPlugin.java  |
| https://developer.android.com/reference/javax/net/ssl/SSLSocket  | io/flutter/plugins/videoplayer/VideoPlayerPlugin.java  |
| https://exoplayer.dev/issues/player-accessed-on-wrong-thread  | l/e/a/a/e2.java  |
| http://dashif.org/guidelines/trickmode  | l/e/a/a/c4/a1/g.java  |
| http://dashif.org/guidelines/last-segment-number  | l/e/a/a/c4/a1/n/d.java  |
| http://dashif.org/guidelines/trickmode  | l/e/a/a/c4/a1/n/d.java  |
| http://www.w3.org/ns/ttml  | l/e/a/a/d4/t/c.java  |
| https://exoplayer.dev/issues/cleartext-not-permitted  | l/e/a/a/f4/d0.java  |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense  | l/e/a/a/w3/l0.java  |
| https://x</LA\_URL>  | l/e/a/a/w3/k0.java  |
| https://x  | l/e/a/a/w3/k0.java  |
| http://ns.adobe.com/xap/1.0/  | l/e/a/a/x3/i0/a.java  |
| https://aomedia.org/emsg/ID3  | l/e/a/a/z3/j/a.java  |
| https://developer.apple.com/streaming/emsg-id3  | l/e/a/a/z3/j/a.java  |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps  | l/e/a/b/a/a/b.java  |
| https://plus.google.com/  | l/e/a/b/d/p/j0.java  |
| http://goo.gl/naFqQk  | l/e/a/b/f/d/d.java  |
| http://goo.gl/8Rd3yj  | l/e/a/b/f/d/l1.java  |
| http://www.google-analytics.com  | l/e/a/b/f/d/v0.java  |
| https://ssl.google-analytics.com  | l/e/a/b/f/d/v0.java  |
| http://goo.gl/8Rd3yj  | l/e/a/b/f/d/y.java  |
| http://hostname/?  | l/e/a/b/i/a.java  |
| https://play.google.com/store/apps/details?id=  | Mogua Engine V1  |
| https://appgallery.cloud.huawei.com  | Mogua Engine V1  |
| https://store.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V1  |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://data-drcn.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dra.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-dre.push.dbankcloud.com  | Mogua Engine V2  |
| https://data-drru.push.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.com  | Mogua Engine V2  |
| https://grs.dbankcloud.cn  | Mogua Engine V2  |
| https://grs.dbankcloud.eu  | Mogua Engine V2  |
| https://grs.dbankcloud.asia  | Mogua Engine V2  |
| https://store1.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store2.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store3.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://store-drru.hispace.hicloud.com/hwmarket/api/  | Mogua Engine V2  |
| https://metrics1.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics-dra.dt.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics2.data.hicloud.com:6447  | Mogua Engine V2  |
| https://metrics5.data.hicloud.com:6447  | Mogua Engine V2  |
| https://www.jsdelivr.com/using-sri-with-dynamic-files  | Mogua Engine V2  |
| https://github.com/apvarun/toastify-js  | Mogua Engine V2  |
| https://github.com/richtr/NoSleep.js/issues/15  | Mogua Engine V2  |
| https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)  | Mogua Engine V2  |
| http://www.w3.org/XML/1998/namespace  | lib/armeabi-v7a/libflutter.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libflutter.so  |
| https://www.w3.org/Style/CSS/Test/Fonts/Ahem/).  | lib/armeabi-v7a/libflutter.so  |
| https://github.com/flutter/flutter/issues.  | lib/armeabi-v7a/libflutter.so  |
| https://okzuixin1118899.oss-cn-beijing.aliyuncs.com/index04.html  | lib/armeabi-v7a/libapp.so  |
| https://ok1112817899.oss-cn-hangzhou.aliyuncs.com/index04.html  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/dart-ui/ChannelBuffers-class.html  | lib/armeabi-v7a/libapp.so  |
| http://www.ibm.com/data/dtd/v11/ibmxhtml1-transitional.dtd  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/svg  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/1998/Math/MathML  | lib/armeabi-v7a/libapp.so  |
| http://www.w3.org/2000/xmlns/  | lib/armeabi-v7a/libapp.so  |
| https://api.flutter.dev/flutter/material/Scaffold/of.html  | lib/armeabi-v7a/libapp.so  |
| https://storage.googleapis.com/okpay/index04.html  | lib/armeabi-v7a/libapp.so  |
| https://www.okpay777.com  | lib/armeabi-v7a/libapp.so  |
| https://oss20231101.okfy8899.com/index04.html  | lib/armeabi-v7a/libapp.so  |
| https://flutter.dev/docs/release/breaking-changes/network-policy-ios-android.  | lib/armeabi-v7a/libapp.so  |
| https://github.com/flutter/flutter/issues/new.  | lib/armeabi-v7a/libapp.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | l/e/a/b/d/c0.java  |
| \_httpparser@13463476.responsepa storationinformation@751124995.fromserial \_double@0150898.fromintege .\_future@4048458.immediate \_growablelist@0150898.\_literal \_link@14069316.fromrawpat c\_growablelist@0150898.withcapaci \_growablelist@0150898.\_literal6 \_receiveportimpl@1026248.fromrawrec -\_list@0150898.\_ofarray z\_timer@1026248.periodic m\_growablelist@0150898.\_literal2 g\_bigintimpl@0150898.from \_list@0150898.empty \_directory@14069316.fromrawpat \_casterror@0150898.\_create l\_invocationmirror@0150898.\_withtype \_colorfilter@16065589.mode \_colorfilter@16065589.srgbtoline i\_rawsocket@14069316.\_writepipe 4\_uri@0150898.file \_growablelist@0150898.\_literal1 q\_imagefilter@16065589.blur \_growablelist@0150898.\_literal4 bb\_growablelist@0150898.\_ofgrowabl x\_growablelist@0150898.of 8n\_routedata@1188504625.ofroute k\_colorfilter@16065589.lineartosr \_nativesocket@14069316.pipe \_cookie@13463476.fromsetcoo authenticationscheme@13463476.fromstring \_list@0150898.of \_list@0150898.generate n\_typeerror@0150898.\_create lectiontoolbarbutton@348392285.text \_list@0150898.\_ofgrowabl \_list@0150898.\_ofefficie \_growablelist@0150898.\_ofarray \_growablelist@0150898.\_literal3 u\_growablelist@0150898.\_ofother \_timer@1026248.\_internal \_growablelist@0150898.\_literal5 \_rawsocket@14069316.\_readpipe \_socket@14069316.\_readpipe \_list@0150898.\_ofother eo\_bytebuffer@7027147.\_new lectiontoolbarbutton@470113492.text ngstreamsubscription@4048458.zoned \_assertionerror@0150898.\_create av\_nativesocket@14069316.normal j\_filestream@14069316.forstdin \_uri@0150898.directory qd\_growablelist@0150898.\_literal8 v\_file@14069316.fromrawpat gh\_growablelist@0150898.generate \_uri@0150898.notsimple 7u\_growablelist@0150898.\_literal7 \_\_growablelist@0150898.\_ofefficie \_future@4048458.immediatee  | lib/armeabi-v7a/libapp.so  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17512775099  | l/e/b/c/a.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=cn, ST=sh, L=sh, O=sh, OU=abcd, CN=abc 签名算法: rsassa\_pkcs1v15 有效期自: 2023-08-10 09:53:37+00:00 有效期至: 2050-12-26 09:53:37+00:00 发行人: C=cn, ST=sh, L=sh, O=sh, OU=abcd, CN=abc 序列号: 0x24eca69b 哈希算法: sha256 md5值: 58ccd18a2db451a6e30a5a558ba6f411 sha1值: a1642cd220a1b4cb897bc4fb61badfb04fe7c830 sha256值: 43517a6e9910c71168fc67b82f4a8f09371e490dcf79a8cd2cb8b1303747efc1 sha512值: 2a4410385863183f1d287c633a540d90b0fbadd5356ca6cc85a42a32626ac44ec3dcc895246b75afd20111b7a9cc31b18523caf24f9a3cc96448ce52ffca9ca6 公钥算法: rsa 密钥长度: 2048 指纹: 859401e99c78efb60c1194e001bb1ec1b4decd5d2195587c98a2fb8dbe2f37ce**

## **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 |
| --- | --- | --- | --- |
| 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\_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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CAMERA | 危险 | 拍照和录像 | 允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像 |
| android.permission.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.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\_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.ACCESS\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_ASSISTED\_GPS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| com.oneworld.onepay.permission.MIPUSH\_RECEIVE | 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 |
| com.oneworld.onepay.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.oneworld.onepay.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.oneworld.onepay.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.oneworld.onepay.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.heytap.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| 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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| android.permission.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.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.leo.okp.MainActivity | **Schemes**: okpay://,  |
| com.leo.okp.mfr.MfrMessageActivity | **Schemes**: agoo://, **Hosts:** com.oneworld.onepay, **Paths:** /thirdpush,  |

**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。**