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

**抖阴（ 5.1.1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 | 抖阴 |
| 版本 | 5.1.1 |
| 包名 | com.wechat.novembertwentythree\_1209 |
| 域名线索 | 44条 |
| URL线索 | 51条 |
| APP图标 |  |
| 分析日期 | 2024年9月8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 | dy\_new\_official\_7rmm5ech2\_5.1.1.apk |
| 文件大小 | 36.74MB |
| MD5值 | eeb7a98a723d239caf55cd0062f8a566 |
| SHA1值 | 9f05fd7e5de0021ed5d312e9e56799759835f475 |
| SHA256值 | 1e189fb9acef846bbd2bba715b61df4283fdbc6483b6ff49fcf38c51ff7cd659 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 抖阴 |
| 包名 | com.wechat.novembertwentythree\_1209 |
| 主活动Activity | com.niming.weipa.ui.splash.SplashActivity |
| 安卓版本名称 | 5.1.1 |
| 安卓版本 | 14 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| mobilegw.aaa.alipay.net | 没有服务器地理信息. |
| g6gsyybak.scen1napib.com | IP: 172.67.204.153  所属国家: United States of America  地区: California  城市: San Francisco |
| pms.mb.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| mobilegw.stable.alipay.net | 没有服务器地理信息. |
| m.alipay.com | IP: 203.209.245.120  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| mdc.html5.qq.com | IP: 125.39.196.199  所属国家: China  地区: Tianjin  城市: Tianjin |
| log.tbs.qq.com | IP: 124.95.231.218  所属国家: China  地区: Liaoning  城市: Shenyang |
| app.dylite.ipx.mx | 没有服务器地理信息. |
| www.u-dictionary.com | IP: 8.219.113.187  所属国家: Singapore  地区: Singapore  城市: Singapore |
| mobilegw-1-64.test.alipay.net | 没有服务器地理信息. |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86  所属国家: China  地区: Shandong  城市: Qingdao |
| openapi-sg.youdao.com | IP: 220.197.31.39  所属国家: China  地区: Jiangsu  城市: Nanjing |
| m.youdao.com | IP: 220.197.31.37  所属国家: China  地区: Jiangsu  城市: Nanjing |
| render.alipay.com | IP: 125.39.47.200  所属国家: China  地区: Tianjin  城市: Tianjin |
| pagead2.googlesyndication.com | IP: 114.250.65.38  所属国家: China  地区: Beijing  城市: Beijing |
| mclient.alipay.com | IP: 125.39.135.57  所属国家: China  地区: Tianjin  城市: Tianjin |
| fanyi-test.youdao.com | IP: 220.197.31.44  所属国家: China  地区: Jiangsu  城市: Nanjing |
| wappaygw.alipay.com | IP: 123.125.216.191  所属国家: China  地区: Beijing  城市: Beijing |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| updateinfo.youdao.com | IP: 220.197.31.39  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mqqad.html5.qq.com | IP: 0.0.0.1  所属国家: -  地区: -  城市: - |
| argus.agoralab.co | IP: 106.14.163.9  所属国家: China  地区: Shanghai  城市: Shanghai |
| debugx5.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| h5.m.taobao.com | IP: 125.38.11.146  所属国家: China  地区: Tianjin  城市: Tianjin |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.potato.im | IP: 108.160.163.108  所属国家: United States of America  地区: California  城市: San Francisco |
| bak.dya9agvmst9v4g825a.com | 没有服务器地理信息. |
| loggw-exsdk.alipay.com | IP: 110.76.6.75  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| api.telegram.org | IP: 199.59.148.246  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |
| bak.dy4x6w27j8wzrue3n4.com | 没有服务器地理信息. |
| openapi.youdao.com | IP: 220.197.31.39  所属国家: China  地区: Jiangsu  城市: Nanjing |
| mobilegw.alipay.com | IP: 203.209.250.8  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.qq.com | IP: 221.198.70.47  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.openssl.org | IP: 34.36.58.177  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| dyfire-01.firebaseio.com | IP: 35.190.39.113  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| app.8dy.me | IP: 122.10.85.4  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| debugtbs.qq.com | IP: 60.29.240.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| app-measurement.com | IP: 114.250.67.33  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: 60.28.172.122  所属国家: China  地区: Tianjin  城市: Tianjin |
| cfg.imtt.qq.com | IP: 60.28.172.238  所属国家: China  地区: Tianjin  城市: Tianjin |
| nb036x.corp.youdao.com | 没有服务器地理信息. |
| mcgw.alipay.com | IP: 123.125.216.192  所属国家: China  地区: Beijing  城市: Beijing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.aaa.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw-1-64.test.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://mobilegw.stable.alipay.net/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/k.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/k.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/k.java |
| http://%s:%d/%s | com/danikula/videocache/m.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/m.java |
| http://%s:%d/%s | com/danikula/videocache/i.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SegmentTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/CommonTabLayout.java |
| http://schemas.android.com/apk/res/android | com/flyco/tablayout/SlidingTabLayout.java |
| https://github.com/lingochamp/FileDownloader/wiki/filedownloader.properties | com/liulishuo/filedownloader/services/a.java |
| http://app.dylite.ipx.mx | com/niming/weipa/a.java |
| http://app.8dy.me | com/niming/weipa/a.java |
| http://app.8dy.me | com/niming/weipa/utils/CommonExtKt.java |
| http://www.qq.com | com/niming/weipa/utils/t.java |
| https://api.telegram.org/bot743083118:AAFcQa9POAvUhMcS2\_AGFR6BKBf\_nj\_vGbE/sendMessage | com/niming/weipa/utils/l.java |
| http://www.qq.com | com/niming/weipa/d/c.java |
| http://www.qq.com | com/niming/weipa/c/a.java |
| http://app.8dy.me | com/niming/weipa/base/BaseActivity.java |
| http://g6gsyybak.scen1napib.com | com/niming/weipa/e/c.java |
| http://bak.dy4x6w27j8wzrue3n4.com | com/niming/weipa/e/c.java |
| http://bak.dya9agvmst9v4g825a.com | com/niming/weipa/e/c.java |
| http://app.dylite.ipx.mx | com/niming/weipa/e/c.java |
| https://api.telegram.org/bot743083118:AAFcQa9POAvUhMcS2\_AGFR6BKBf\_nj\_vGbE/sendMessage | com/niming/weipa/e/b.java |
| https://github.com/yyued/SVGAPlayer-Android | com/slzhibo/library/ui/view/widget/svga/SVGAParser.java |
| https://www.potato.im/p/androids | com/slzhibo/library/ui/view/dialog/WebViewDialog.java |
| https://www.potato.im/p/androids | com/slzhibo/library/ui/activity/home/WebViewActivity.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/l.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/m.java |
| https://log.tbs.qq.com/ajax?c=pu&tk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=dl&k= | com/tencent/smtt/utils/m.java |
| https://cfg.imtt.qq.com/tbs?v=2&mk= | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k= | com/tencent/smtt/utils/m.java |
| https://mqqad.html5.qq.com/adjs | com/tencent/smtt/utils/m.java |
| https://log.tbs.qq.com/ajax?c=ucfu&k= | com/tencent/smtt/utils/m.java |
| https://tbsrecovery.imtt.qq.com/getconfig | com/tencent/smtt/utils/m.java |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs | com/tencent/smtt/utils/d.java |
| http://www.u-dictionary.com/home/word/%s/from/ | com/youdao/sdk/app/h.java |
| http://m.youdao.com/dict?le=%s&q=%s | com/youdao/sdk/app/h.java |
| http://updateinfo.youdao.com/update? | com/youdao/sdk/app/a.java |
| http://openapi-sg.youdao.com/log | com/youdao/sdk/app/other/e.java |
| http://openapi.youdao.com/log | com/youdao/sdk/app/other/e.java |
| http://openapi-sg.youdao.com | com/youdao/sdk/ydonlinetranslate/other/e.java |
| http://openapi.youdao.com | com/youdao/sdk/ydonlinetranslate/other/e.java |
| http://openapi-sg.youdao.com | com/youdao/sdk/ydonlinetranslate/other/b.java |
| http://nb036x.corp.youdao.com:8681 | com/youdao/sdk/ydonlinetranslate/other/b.java |
| http://openapi-sg.youdao.com | com/youdao/sdk/ydonlinetranslate/other/g.java |
| http://openapi.youdao.com | com/youdao/sdk/ydonlinetranslate/other/g.java |
| http://fanyi-test.youdao.com/translate\_a?q= | com/youdao/sdk/ydonlinetranslate/other/g.java |
| https://mobilegw.alipay.com/mgw.htm | e/a/b/c/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | e/a/b/c/a.java |
| https://mcgw.alipay.com/sdklog.do | e/a/b/c/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | e/a/b/c/a.java |
| http://m.alipay.com/?action=h5quit | e/a/b/c/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | e/a/b/c/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | e/a/b/c/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | e/a/b/d/a.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | e/c/a/a/b/a/b.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/a.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/q.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/i0.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/j.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | io/reactivex/z.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | io/reactivex/exceptions/OnErrorNotImplementedException.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | io/reactivex/exceptions/UndeliverableException.java |
| https://dyfire-01.firebaseio.com | 摸瓜V1引擎 |
| app-measurement.com | 摸瓜V3引擎 |
| http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s | lib/armeabi-v7a/libagora-rtc-sdk.so |
| http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s | lib/armeabi-v7a/libagora-rtc-sdk.so |
| http://sQUIC | lib/armeabi-v7a/libagora-rtc-sdk.so |
| http://www.openssl.org/support/faq.html | lib/armeabi-v7a/libfqffmpeg.so |
| http://s | lib/armeabi-v7a/libsaturn.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/k.java |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libfqplayer.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | com/tomato/ijk/media/player/IjkMediaMeta.java |
| 17179869184 | tv/danmaku/ijk/media/player/i.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=00, ST=pp, L=pp, O=xsl, OU=xsl, CN=xsl 签名算法: rsassa\_pkcs1v15 有效期自: 2019-03-05 03:33:31+00:00 有效期至: 2069-02-20 03:33:31+00:00 发行人: C=00, ST=pp, L=pp, O=xsl, OU=xsl, CN=xsl 序列号: 0x7f494ee4 哈希算法: sha256 md5值: 2c1be98a39dc70e7b4b111127b3ba5de sha1值: 24bcecac061c7701f2c4bf078ae8eb384211d78a sha256值: 67f76e5d217a30a91b5a08f96cff949dce57718e5f1607bec24a4c191ae8aae0 sha512值: df46ef6eab567df40d81750ca824454899bdff3a556ac3d50747ef2b7b86f9fc50205742144cceff67c3b8b3b345408e0489bb9d80c644dcab9ac8463ca2f317 公钥算法: rsa 密钥长度: 2048 指纹: da5f6dfaa4dd7458e4d7b1883469ab5a9f32f2e16636e0179ffdb463559304a1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "anonymous\_user" : "老湿" |
| "be\_gesture\_password" : "密码锁" |
| "firebase\_database\_url" : "https://dyfire-01.firebaseio.com" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>购买用户：</font>%1$s" |
| "fq\_not\_login\_user" : "未登录用户" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "私有座驾，您暂不符合购买条件" |
| "fq\_secret" : "私密" |
| "google\_api\_key" : "AIzaSyAPpyowD\_8PwYOJXOupAv2XaiI\_aflJCfc" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyAPpyowD\_8PwYOJXOupAv2XaiI\_aflJCfc" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>User purchase：</font>%1$s" |
| "fq\_not\_login\_user" : "Unlogged user" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "Private car, you do not meet the purchase conditions" |
| "fq\_secret" : "Private" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>购买用户：</font>%1$s" |
| "fq\_not\_login\_user" : "未登录用户" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "私有座驾，您暂不符合购买条件" |
| "fq\_secret" : "私密" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>购买用户：</font>%1$s" |
| "fq\_not\_login\_user" : "未登录用户" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "私有座驾，您暂不符合购买条件" |
| "fq\_secret" : "密密" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>购买用户：</font>%1$s" |
| "fq\_not\_login\_user" : "未登录用户" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "私有座驾，您暂不符合购买条件" |
| "fq\_secret" : "사적인" |
| "fq\_anchor\_auth\_success\_tips" : "恭喜您，通过了主播认证" |
| "fq\_auth\_helper\_download\_tips" : "为了方便您获得极致的开播体验， 请下载独立开播助手" |
| "fq\_fast\_auth\_login" : "授权登录" |
| "fq\_hd\_gift\_password" : "礼物口令" |
| "fq\_no\_operation\_authority" : "无操作权限" |
| "fq\_no\_operation\_authority\_tips" : "您当前没有开启并设置付费直播间的权限，详情请咨询管理员。" |
| "fq\_nobility\_open\_buy\_user" : "<font color=#878787>购买用户：</font>%1$s" |
| "fq\_not\_login\_user" : "未登录用户" |
| "fq\_pk\_total\_session" : "总PK场次" |
| "fq\_pk\_victory\_session" : "获胜场次" |
| "fq\_private\_car" : "私有" |
| "fq\_private\_car\_buy\_tips" : "私有座驾，您暂不符合购买条件" |
| "fq\_secret" : "私密" |

## **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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.qti.permission.PROFILER | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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\_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.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.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 |
| com.google.android.finsky.permission.BIND\_GET\_INSTALL\_REFERRER\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| 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 |

## **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。**