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

**aidum（ 1.0.73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 | aidum |
| 版本 | 1.0.73 |
| 包名 | com.freelan.chat |
| 域名线索 | 50条 |
| URL线索 | 29条 |
| APP图标 |  |
| 分析日期 | 2025年5月17日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | freelan.apk |
| 文件大小 | 71.0MB |
| MD5值 | 2c93035ff3c8b2fb221a924b9eaf60d1 |
| SHA1值 | 6dc5e852ac1c160a2335d7277217c549cb9b95a4 |
| SHA256值 | c1787f53d35aa5cc8bfe5f67750de594d97c68a1f9c3b3500a3a4b1a33060320 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | aidum |
| 包名 | com.freelan.chat |
| 主活动Activity | com.freelan.chat.MainActivity |
| 安卓版本名称 | 1.0.73 |
| 安卓版本 | 10073 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| imjk.ccqsjimjk.cc | IP: 16.163.243.145  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| plbslog.umeng.com | IP: 36.156.202.68  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| ulogs.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| frljk.lqhljk.vip | IP: 43.199.104.44  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| frljk.jkkahbsl.com | IP: 43.198.61.166  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| ouplog.umeng.com | IP: 47.246.110.93  所属国家: Singapore  地区: Singapore  城市: Singapore |
| frljk.imjk77live.com | IP: 108.136.36.245  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| px.ucweb.com | IP: 116.132.217.241  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| developer.umeng.com | IP: 59.82.112.112  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| frljk.jknxbzvag.com | IP: 18.166.127.62  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| imjk.ccqsjimjk.vip | IP: 18.167.122.15  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| ce3e75d5.jpush.cn | IP: 120.233.50.89  所属国家: China  地区: Guangdong  城市: Shenzhen |
| freelantv.oss-cn-hongkong.aliyuncs.com | IP: 47.79.64.233  所属国家: United States of America  地区: California  城市: San Mateo |
| alogsus.umeng.com | IP: 223.109.148.177  所属国家: China  地区: Jiangsu  城市: Nanjing |
| xml.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| alogus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| imjk.ccqsjimjk.com | IP: 16.163.243.145  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| freelan-1307976365.cos.accelerate.myqcloud.com | IP: 111.202.29.114  所属国家: China  地区: Beijing  城市: Beijing |
| errlog.umeng.com | IP: 223.109.148.142  所属国家: China  地区: Jiangsu  城市: Nanjing |
| frljk.jkmansvx.com | IP: 43.199.115.215  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| 139.224.238.21 | IP: 139.224.238.21  所属国家: China  地区: Shanghai  城市: Shanghai |
| upload-z2.qiniup.com | IP: 163.142.153.213  所属国家: China  地区: Guangdong  城市: Foshan |
| playready.directtaps.net | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| frljk.jksenabbbuu.com | IP: 18.166.127.62  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| greenrobot.org | IP: 85.13.163.69  所属国家: Germany  地区: Thuringen  城市: Friedersdorf |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| imjk.jalaimbk.vip | IP: 16.78.142.246  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| freemarker.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.slf4j.org | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| sdkapi-smartop.jiguang.cn | 没有服务器地理信息. |
| frljk.jkoensba.com | IP: 43.199.89.49  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| frljk.77liveimjk.com | IP: 43.218.169.233  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| frljk.lqhlim.vip | IP: 43.198.134.102  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| ulogs.umengcloud.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| api.m.taobao.com | 没有服务器地理信息. |
| imjk.ccqsjimjk.net | IP: 43.199.116.98  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| frljk.lqhlim.cc | IP: 43.198.29.174  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| imjk.jalaimbk.cc | IP: 43.218.108.125  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| px-intl.ucweb.com | IP: 157.185.188.1  所属国家: Canada  地区: Ontario  城市: North York |
| pslog.umeng.com | IP: 59.82.29.162  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| frljk.lqhljk.cc | IP: 43.198.4.186  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| freemarker.org | IP: 192.64.119.217  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| www.webrtc.org | IP: 172.217.14.238  所属国家: United States of America  地区: California  城市: Mountain View |
| frljk.imjk77live.top | IP: 43.218.169.233  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| cc.frl2022.net | IP: 119.28.184.74  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| schemas.microsoft.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| frljk.imjk77live.net | IP: 108.136.36.245  所属国家: Indonesia  地区: Jakarta Raya  城市: Jakarta |
| aaid.umeng.com | IP: 223.109.148.171  所属国家: China  地区: Jiangsu  城市: Nanjing |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://sdkapi-smartop.jiguang.cn | cn/jiguang/be/c.java |
| https://ce3e75d5.jpush.cn/wi/op8jdu | cn/jiguang/s/c.java |
| https://upload-z2.qiniup.com | cn/jiguang/bf/a.java |
| http://xml.apache.org/xslt | com/blankj/utilcode/util/LogUtils.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://freelantv.oss-cn-hongkong.aliyuncs.com/domain.config | com/fim/lib/http/RetrofitMgr.java |
| https://freelan-1307976365.cos.accelerate.myqcloud.com/domain.config | com/fim/lib/http/RetrofitMgr.java |
| http://cc.frl2022.net:19527 | com/fim/lib/http/RetrofitMgr.java |
| http://api.m.taobao.com/rest/api3.do?api=mtop.common.getTimestamp | com/fim/lib/utils/TimeUtil.java |
| https://errlogos.umeng.com/upload | com/uc/crashsdk/e.java |
| https://errlog.umeng.com/upload | com/uc/crashsdk/e.java |
| https://px-intl.ucweb.com | com/uc/crashsdk/a/h.java |
| https://px.ucweb.com | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlog.umeng.com/api/crashsdk/logcollect | com/uc/crashsdk/a/h.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.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://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://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://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://freemarker.apache.org/docs/ref\_builtins.html; | freemarker/core/BuiltIn.java |
| http://freemarker.org/docs/ref\_directive\_list.html). | freemarker/core/FMParserTokenManager.java |
| http://freemarker.org/docs/ref\_directive\_alphaidx.html; | freemarker/core/FMParserTokenManager.java |
| https://greenrobot.org/greendao/documentation/database-encryption/ | org/greenrobot/greendao/database/DatabaseOpenHelper.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | org/java\_websocket/AbstractWebSocket.java |
| http://playready.directtaps.net/pr/svc/rightsmanager.asmx | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | tv/danmaku/ijk/media/exo/demo/SmoothStreamingTestMediaDrmCallback.java |
| https://frljk.jkkahbsl.com | 摸瓜V2引擎 |
| https://frljk.jkmansvx.com | 摸瓜V2引擎 |
| https://frljk.jknxbzvag.com | 摸瓜V2引擎 |
| https://frljk.jkoensba.com | 摸瓜V2引擎 |
| https://frljk.jksenabbbuu.com | 摸瓜V2引擎 |
| https://frljk.lqhlim.vip | 摸瓜V2引擎 |
| https://frljk.lqhljk.vip | 摸瓜V2引擎 |
| https://frljk.lqhljk.cc | 摸瓜V2引擎 |
| https://frljk.lqhlim.cc | 摸瓜V2引擎 |
| https://imjk.ccqsjimjk.cc | 摸瓜V2引擎 |
| https://imjk.ccqsjimjk.net | 摸瓜V2引擎 |
| https://imjk.ccqsjimjk.com | 摸瓜V2引擎 |
| https://imjk.ccqsjimjk.vip | 摸瓜V2引擎 |
| https://frljk.imjk77live.com | 摸瓜V2引擎 |
| https://frljk.imjk77live.top | 摸瓜V2引擎 |
| https://frljk.imjk77live.net | 摸瓜V2引擎 |
| https://frljk.77liveimjk.com | 摸瓜V2引擎 |
| https://imjk.jalaimbk.vip | 摸瓜V2引擎 |
| https://imjk.jalaimbk.cc | 摸瓜V2引擎 |
| http://agoratest | lib/arm64-v8a/libagora-rtc-sdk.so |
| http://139.224.238.21:9090/udrm/udrmGetLicense | lib/arm64-v8a/libagora-rtc-sdk.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor | lib/arm64-v8a/libagora-rtc-sdk.so |
| http://s | lib/arm64-v8a/libagora-rtc-sdk.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| appro@openssl.org | lib/arm64-v8a/libagora-ffmpeg.so |
| appro@openssl.org | lib/arm64-v8a/libagora-rtc-sdk.so |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869185 | freemarker/core/FMParserTokenManager.java |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: CN=freelan 签名算法: rsassa\_pkcs1v15 有效期自: 2020-05-05 06:46:49+00:00 有效期至: 2045-04-29 06:46:49+00:00 发行人: CN=freelan 序列号: 0x7a0e4207 哈希算法: sha256 md5值: 61cfee4075d959392aa22e8ea8ec00ac sha1值: 990a6a49ac2f817cc6f392ba3ed825b8064fbd3d sha256值: 7ac3162c4199e72f86b3eedca9c46b60cdfe3a592c835a4a0e07d0bc97f01929 sha512值: f39a7ce2091560dcc6a6c93f8cb0b1cf47d032128f8514c5e743f3fb9c02f78d3606ad8ac20b740a75e2e465f0f9f744b22775455320b53c962332dad6d86edc 公钥算法: rsa 密钥长度: 2048 指纹: a8f724481455266fc02c24cc255f50a7f177658665a5b318473e82dcff4c1877**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "allBlackUser" : "共%1$s位黑名单好友" |
| "allUser" : "所有人" |
| "ask\_pay\_password" : "未设置支付密码？" |
| "awserNum" : "条回复>" |
| "awseryouquest" : "运营团队已经收到您的投诉信息，将在24小时内给与答复" |
| "blackUser" : "拉黑此联系人" |
| "chat\_private" : "私密聊天" |
| "complainUser" : "投诉该用户" |
| "containKey" : "包含" |
| "enterPwd" : "输入密码" |
| "enterPwdAgain" : "请输入确认密码" |
| "find\_password" : "找回密码" |
| "forgetPassword" : "忘记密码?" |
| "forget\_password" : "忘记密码" |
| "google\_api\_key" : "AIzaSyDYWpA4OHy4Zk7V7yPS\_t2qZtcq2teGqL0" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyDYWpA4OHy4Zk7V7yPS\_t2qZtcq2teGqL0" |
| "illegalAuthorization" : "非法授权" |
| "inputLoginPwd" : "请输入登录密码" |
| "inputPassword" : "请输入密码" |
| "loginPwd" : "登录密码" |
| "mdyPayPassword" : "修改支付密码" |
| "mdy\_password" : "修改密码" |
| "noSetPassword" : "未设置密码" |
| "password" : "密码" |
| "payPassword" : "支付密码" |
| "please\_input\_password" : "请输入密码" |
| "pwdLeastSixChar" : "密码不能少于6位" |
| "pwdNeedSixNum" : "支付密码需六位数字" |
| "pwdNeedSixNumber" : "密码至少需要6位数字" |
| "search\_user" : "搜索用户" |
| "setPayPassword" : "设置支付密码" |
| "set\_password" : "设置密码" |
| "signPrivate" : "个性签名" |
| "userName" : "用户名" |
| "allBlackUser" : "Total %1$s Teman yang Diblokir" |
| "allUser" : "Semua Orang" |
| "ask\_pay\_password" : "Belum mengatur kata sandi pembayaran?" |
| "awserNum" : "Balasan" |
| "awseryouquest" : "Tim operasional telah menerima informasi keluhan Anda dan akan memberikan tanggapan dalam waktu 24 jam" |
| "blackUser" : "Blokir kontak ini" |
| "chat\_private" : "Chat pribadi" |
| "complainUser" : "Kompilasi pengguna ini" |
| "containKey" : "Mengandung" |
| "enterPwd" : "Masukkan kata sandi" |
| "enterPwdAgain" : "Masukkan konfirmasi kata sandi" |
| "find\_password" : "Pulihkan Kata Sandi" |
| "forgetPassword" : "Lupa kata sandi?" |
| "forget\_password" : "Lupa Kata Sandi" |
| "illegalAuthorization" : "Otorisasi ilegal" |
| "inputLoginPwd" : "Masukkan kata sandi login" |
| "inputPassword" : "Masukkan kata sandi" |
| "loginPwd" : "Kata Sandi Masuk" |
| "mdyPayPassword" : "Ubah kata sandi pembayaran" |
| "mdy\_password" : "Ubah Kata Sandi" |
| "noSetPassword" : "Sandi belum diatur" |
| "password" : "Kata sandi" |
| "payPassword" : "Kata sandi pembayaran" |
| "please\_input\_password" : "Masukkan kata sandi" |
| "pwdLeastSixChar" : "Kata sandi tidak boleh kurang dari 6 karakter" |
| "pwdNeedSixNum" : "Kata sandi pembayaran harus terdiri dari enam digit" |
| "pwdNeedSixNumber" : "Kata sandi harus terdiri dari setidaknya 6 digit" |
| "search\_user" : "Cari pengguna" |
| "setPayPassword" : "Atur kata sandi pembayaran" |
| "set\_password" : "Atur Kata Sandi" |
| "signPrivate" : "Tanda tangan pribadi" |
| "userName" : "Nama Pengguna" |
| "allBlackUser" : "共%1$s位黑名单好友" |
| "allUser" : "所有人" |
| "ask\_pay\_password" : "未设置支付密码？" |
| "awserNum" : "条回复>" |
| "awseryouquest" : "运营团队已经收到您的投诉信息，将在24小时内给与答复" |
| "blackUser" : "拉黑此联系人" |
| "chat\_private" : "私密聊天" |
| "complainUser" : "投诉该用户" |
| "containKey" : "包含" |
| "enterPwd" : "输入密码" |
| "enterPwdAgain" : "请输入确认密码" |
| "find\_password" : "找回密码" |
| "forgetPassword" : "忘记密码?" |
| "forget\_password" : "忘记密码" |
| "illegalAuthorization" : "非法授权" |
| "inputLoginPwd" : "请输入登录密码" |
| "inputPassword" : "请输入密码" |
| "loginPwd" : "登录密码" |
| "mdyPayPassword" : "修改支付密码" |
| "mdy\_password" : "修改密码" |
| "noSetPassword" : "未设置密码" |
| "password" : "密码" |
| "payPassword" : "支付密码" |
| "please\_input\_password" : "请输入密码" |
| "pwdLeastSixChar" : "密码不能少于6位" |
| "pwdNeedSixNum" : "支付密码需六位数字" |
| "pwdNeedSixNumber" : "密码至少需要6位数字" |
| "search\_user" : "搜索用户" |
| "setPayPassword" : "设置支付密码" |
| "set\_password" : "设置密码" |
| "signPrivate" : "个性签名" |
| "userName" : "用户名" |
| "allBlackUser" : "Total of %1$s blacklisted friends" |
| "allUser" : "Everyone" |
| "ask\_pay\_password" : "Payment password not set?" |
| "awserNum" : "Replies" |
| "awseryouquest" : "The operations team has received your complaint and will respond within 24 hours" |
| "blackUser" : "Block" |
| "chat\_private" : "Private Chat" |
| "complainUser" : "Report User" |
| "containKey" : "Contains" |
| "enterPwd" : "Enter Password" |
| "enterPwdAgain" : "Re-enter Password" |
| "find\_password" : "Recover Password" |
| "forgetPassword" : "Forgot Password?" |
| "forget\_password" : "Forgot Password" |
| "illegalAuthorization" : "Illegal Authorization" |
| "inputLoginPwd" : "Enter Login Password" |
| "inputPassword" : "Please Enter Password" |
| "loginPwd" : "Login Password" |
| "mdyPayPassword" : "Change Payment Password" |
| "mdy\_password" : "Change Password" |
| "noSetPassword" : "Password Not Set" |
| "password" : "Password" |
| "payPassword" : "Payment password" |
| "please\_input\_password" : "Please Enter Password" |
| "pwdLeastSixChar" : "Password cannot be less than 6 characters" |
| "pwdNeedSixNum" : "Payment password must be six digits" |
| "pwdNeedSixNumber" : "Password must be at least 6 digits" |
| "search\_user" : "Search User" |
| "setPayPassword" : "Set Payment Password" |
| "set\_password" : "Set Password" |
| "signPrivate" : "Personal Signature" |
| "userName" : "Username" |
| "allBlackUser" : "Total %1$s Teman yang Diblokir" |
| "allUser" : "Semua Orang" |
| "ask\_pay\_password" : "Belum mengatur kata sandi pembayaran?" |
| "awserNum" : "Balasan" |
| "awseryouquest" : "Tim operasional telah menerima informasi keluhan Anda dan akan memberikan tanggapan dalam waktu 24 jam" |
| "blackUser" : "Blokir kontak ini" |
| "chat\_private" : "Chat pribadi" |
| "complainUser" : "Kompilasi pengguna ini" |
| "containKey" : "Mengandung" |
| "enterPwd" : "Masukkan kata sandi" |
| "enterPwdAgain" : "Masukkan konfirmasi kata sandi" |
| "find\_password" : "Pulihkan Kata Sandi" |
| "forgetPassword" : "Lupa kata sandi?" |
| "forget\_password" : "Lupa Kata Sandi" |
| "illegalAuthorization" : "Otorisasi ilegal" |
| "inputLoginPwd" : "Masukkan kata sandi login" |
| "inputPassword" : "Masukkan kata sandi" |
| "loginPwd" : "Kata Sandi Masuk" |
| "mdyPayPassword" : "Ubah kata sandi pembayaran" |
| "mdy\_password" : "Ubah Kata Sandi" |
| "noSetPassword" : "Sandi belum diatur" |
| "password" : "Kata sandi" |
| "payPassword" : "Kata sandi pembayaran" |
| "please\_input\_password" : "Masukkan kata sandi" |
| "pwdLeastSixChar" : "Kata sandi tidak boleh kurang dari 6 karakter" |
| "pwdNeedSixNum" : "Kata sandi pembayaran harus terdiri dari enam digit" |
| "pwdNeedSixNumber" : "Kata sandi harus terdiri dari setidaknya 6 digit" |
| "search\_user" : "Cari pengguna" |
| "setPayPassword" : "Atur kata sandi pembayaran" |
| "set\_password" : "Atur Kata Sandi" |
| "signPrivate" : "Tanda tangan pribadi" |
| "userName" : "Nama Pengguna" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 此APP的危险动作**

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.READ\_PHONE\_STATE | 危险 | 读取电话状态和身份 | 允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等 |
| android.permission.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.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| 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.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.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.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.CHANGE\_WIFI\_MULTICAST\_STATE | 正常 | 允许Wi-Fi多播接收 | 允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率 |
| android.permission.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| android.permission.WAKE\_LOCK | 正常 | 防止手机睡眠 | 允许应用程序防止手机进入睡眠状态 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CAPTURE\_AUDIO\_OUTPUT | 系统需要 |  | 允许应用程序捕获音频输出。 |
| android.permission.CAPTURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获视频输出 |
| android.permission.CAPTURE\_SECURE\_VIDEO\_OUTPUT | 正常 |  | 允许应用程序捕获安全视频输出 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERACT\_ACROSS\_USERS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_CACHE\_FILESYSTEM | 系统需要 | 访问缓存文件系统 | 允许应用程序读取和写入缓存文件系统 |
| 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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.POST\_NOTIFICATIONS | 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 |
| com.google.android.gms.permission.AD\_ID | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.freelan.chat.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |
| android.permission.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 |
| 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\_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.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.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.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.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。**