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

**Ladbrokes（ 5.4.0119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 | Ladbrokes |
| 版本 | 5.4.0119 |
| 包名 | com.lb7be |
| 域名线索 | 33条 |
| URL线索 | 48条 |
| APP图标 |  |
| 分析日期 | 2025年6月30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 | LADBROKES\_599.apk |
| 文件大小 | 89.96MB |
| MD5值 | 414cefd1f960ee1b0e9d1a91a80597a7 |
| SHA1值 | 4a6a6da7e3fe20ac79e157e05762999fcf7ad877 |
| SHA256值 | 785859a62f4f53d0bcbe68fbdf8d08fe1302eb1357f2323fdff85579b32b24eb |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Ladbrokes |
| 包名 | com.lb7be |
| 主活动Activity | com.qsf.taogin.Splash.vi.SplashActivity |
| 安卓版本名称 | 5.4.0119 |
| 安卓版本 | 599 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errlogos.umeng.com | IP: 47.246.110.96  所属国家: Singapore  地区: Singapore  城市: Singapore |
| errnewlog.umeng.com | IP: 223.109.148.129  所属国家: China  地区: Jiangsu  城市: Nanjing |
| live.leisu.com | IP: 27.221.79.6  所属国家: China  地区: Shandong  城市: Qingdao |
| ccs.umeng.com | IP: 110.253.189.138  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| 2021euapi.k33uc.com | 没有服务器地理信息. |
| errnewlogos.umeng.com | IP: 47.246.110.18  所属国家: Singapore  地区: Singapore  城市: Singapore |
| developer.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| www.jihai8.com | IP: 47.95.126.66  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| errlog.umeng.com | IP: 223.109.148.180  所属国家: China  地区: Jiangsu  城市: Nanjing |
| tg.zjqde.cn | 没有服务器地理信息. |
| alogus.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| plbslog.umeng.com | IP: 36.156.202.78  所属国家: China  地区: Jiangsu  城市: Yangzhou |
| utoken.umeng.com | IP: 223.109.148.139  所属国家: China  地区: Jiangsu  城市: Nanjing |
| pslog.umeng.com | IP: 59.82.31.92  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| schemas.android.com | 没有服务器地理信息. |
| h.trace.qq.com | IP: 113.56.189.162  所属国家: China  地区: Hubei  城市: Huangshi |
| ip-api.com | IP: 208.95.112.1  所属国家: United States of America  地区: North Carolina  城市: Skyland |
| www.slf4j.org | IP: 159.100.250.151  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| audid.umeng.com | IP: 123.183.232.13  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| msg.umengcloud.com | IP: 110.253.188.231  所属国家: China  地区: Hebei  城市: Zhangjiakou |
| ulogs.umengcloud.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| app.reflpo.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| app.tpxdrme.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| sss.umeng.com | IP: 59.82.29.249  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| ulogs.umeng.com | IP: 223.109.148.130  所属国家: China  地区: Jiangsu  城市: Nanjing |
| cs.cs3upebmh9.shop | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| c.k33uc.com | 没有服务器地理信息. |
| offmsg.umeng.com | IP: 59.82.31.154  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| alogsus.umeng.com | IP: 223.109.148.179  所属国家: China  地区: Jiangsu  城市: Nanjing |
| m1.lbzz15786.art | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| www.tgtop88.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| 43.132.55.55 | IP: 43.132.55.55  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://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/f/c.java |
| https://errnewlogos.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://errnewlog.umeng.com/api/crashsdk/logcollect | com/efs/sdk/base/core/controller/ControllerCenter.java |
| https://github.com/danikula/AndroidVideoCache/issues/88. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues/43. | com/danikula/videocache/HttpUrlSource.java |
| https://github.com/danikula/AndroidVideoCache/issues. | com/danikula/videocache/HttpUrlSource.java |
| http://%s:%d/%s | com/danikula/videocache/f.java |
| https://github.com/danikula/AndroidVideoCache/issues/134. | com/danikula/videocache/f.java |
| http://%s:%d/%s | com/danikula/videocache/HttpProxyCacheServer.java |
| https://app.tpxdrme.cn/info/erefs | com/qsf/taogin/SubNetSettings.java |
| https://www.jihai8.com/zq/ | com/qsf/taogin/MainActivity.java |
| https://live.leisu.com | com/qsf/taogin/MainActivity.java |
| https://c.k33uc.com/?lang= | com/qsf/taogin/MainActivity.java |
| http://ip-api.com/ | com/qsf/taogin/api/RetrofitClient.java |
| https://app.reflpo.cn/info/dpeek/Android.html | com/qsf/taogin/api/HeaderInterceptor.java |
| https://2021euapi.k33uc.com/api/ | com/qsf/taogin/bigMatch/api/BigMatchLiveRetrofitManager.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/bigMatch/home/BigMatchHomeCirleView.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/market/barchart/BarView.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/home/vi/CirleView.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/utility/DrawCicler.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/utility/DrawCiclerX.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/utility/AllenCommonTabLayoutV2.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/utility/AllenSlidingTabLayout.java |
| http://schemas.android.com/apk/res/android | com/qsf/taogin/utility/AllenCommonTabLayoutV3.java |
| https://tg.zjqde.cn/ | com/qsf/taogin/utility/CS\_contact.java |
| https://cs.cs3upebmh9.shop/qsf/iframe/user/login | com/qsf/taogin/utility/CS\_contact.java |
| https://www.tgtop88.com/ | com/qsf/taogin/account/view/AccountMainV2Fragment.java |
| https://2021euapi.k33uc.com/api/?token= | com/qsf/taogin/websocket/BigMatchWebSocketManager.java |
| https://m1.lbzz15786.art | com/qsf/taogin/Splash/vi/SplashActivity.java |
| http://developer.umeng.com/docs/66650/cate/66650 | com/umeng/analytics/pro/j.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://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://alogus.umeng.com | com/umeng/commonsdk/stateless/a.java |
| https://offmsg.umeng.com/v2/offmsg/switch | com/umeng/message/proguard/ai.java |
| https://offmsg.umeng.com/v2/offmsg/req | com/umeng/message/proguard/s.java |
| https://msg.umengcloud.com/v3/tag/add | com/umeng/message/proguard/an.java |
| https://msg.umengcloud.com/v3/tag/delete | com/umeng/message/proguard/an.java |
| https://msg.umengcloud.com/v3/tag/get | com/umeng/message/proguard/an.java |
| https://ccs.umeng.com/aa | com/umeng/message/proguard/o.java |
| https://sss.umeng.com/api/v2/al | com/umeng/message/proguard/o.java |
| https://msg.umengcloud.com/admsg/v3/stats | com/umeng/message/proguard/ag.java |
| https://msg.umengcloud.com/admsg/v3/launch | com/umeng/message/proguard/ag.java |
| https://msg.umengcloud.com/admsg/v3/getmsg | com/umeng/message/proguard/ag.java |
| https://msg.umengcloud.com/v3/alias/set | com/umeng/message/proguard/x.java |
| https://msg.umengcloud.com/v3/alias/delete | com/umeng/message/proguard/x.java |
| https://msg.umengcloud.com/v3/alias | com/umeng/message/proguard/x.java |
| https://audid.umeng.com/v3/a/audid/req | com/umeng/ut/a/b/g.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrashContent.java |
| https://errnewlogos.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlogos.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com/upload | com/umeng/umcrash/UMCrash.java |
| https://errnewlog.umeng.com | com/umeng/umcrash/UMCrash.java |
| https://utoken.umeng.com/api/postZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://utoken.umeng.com/api/updateZdata/v4 | com/umeng/umzid/ZIDManager.java |
| https://errlog.umeng.com | com/uc/crashsdk/a/d.java |
| https://errlogos.umeng.com | com/uc/crashsdk/a/d.java |
| http://43.132.55.55/conf?id= | com/tencent/msdk/dns/core/a.java |
| http://%s/d?%s&alg=des | com/tencent/msdk/dns/core/n/b/c.java |
| http://%s/d?%s&alg=aes | com/tencent/msdk/dns/core/n/a/c.java |
| https://h.trace.qq.com/kv?attaid=0ac00073068&token=9663669547&carrier= | com/tencent/msdk/dns/d/a.java |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection | org/java\_websocket/AbstractWebSocket.java |
| http://www.slf4j.org/codes.html | org/slf4j/MDC.java |
| http://www.slf4j.org/codes.html | org/slf4j/LoggerFactory.java |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| danikula@gmail.com | com/danikula/videocache/HttpUrlSource.java |
| this@calendarfragment.requirecon | com/qsf/taogin/micronet/view/CalendarFragment.java |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: False v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: C=6CrK7S7g6CrK7S7g, ST=EuCS8MXbEuCS8MXb, L=Rt4aQH36Rt4aQH36, O=cwpWWy4gcwpWWy4g, OU=BKUp3P8UBKUp3P8U, CN=qQ8rz7VMqQ8rz7VM 签名算法: rsassa\_pkcs1v15 有效期自: 2019-01-29 07:26:46+00:00 有效期至: 2069-01-16 07:26:46+00:00 发行人: C=6CrK7S7g6CrK7S7g, ST=EuCS8MXbEuCS8MXb, L=Rt4aQH36Rt4aQH36, O=cwpWWy4gcwpWWy4g, OU=BKUp3P8UBKUp3P8U, CN=qQ8rz7VMqQ8rz7VM 序列号: 0x2e7192d1 哈希算法: sha256 md5值: 452e1fb91a108f4fc362961c57b9e2f2 sha1值: ac48a0d77f26d779b6ab7ca9a5ad9d8b7f0211ec sha256值: a5cf03565f33ad1052d3f9ec4cff9280c272e55af7f11a1f3e256208aca5dd99 sha512值: 4374799803aa4f121c0d030514c9003684d4c6f932512fe2cdc2496096d4137c37463a060d4c996f72ee371d85b15541abf53832548c2b5f88ccf6af96cf3899 公钥算法: rsa 密钥长度: 2048 指纹: baa107bff257cc875c6f2a07d532c67e7f08adc9b1a817741d0ec009d4c08eab**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "STR\_KEY" : "STR\_FROM\_RESOURCE\_VALUE" |
| "auto\_authorization\_description" : "不想错过任何一个获利机会，请授权K7系统自动执行" |
| "auto\_authorization\_description2" : "每次下单时，授权K7系统自动执行" |
| "ball\_possession" : "控球率" |
| "cancel\_authorization" : "取消授权" |
| "dialog\_auth\_method\_mail" : "邮箱" |
| "dialog\_auth\_method\_mail\_common" : "邮箱:" |
| "dialog\_auth\_method\_mobile" : "手机" |
| "dialog\_choose\_auth" : "验证方式" |
| "dialog\_choose\_auth\_common" : "验证方式" |
| "draw\_password" : "提领密码 :" |
| "fingerprint\_auth" : "进行指纹登入" |
| "fingerprint\_auth\_not\_ready" : "指纹辨识未设定完成" |
| "fingerprint\_auth\_successful" : "指纹辨识成功" |
| "guide\_user\_name" : "麦可麦可麦…" |
| "inout\_password" : "输入密码" |
| "login\_password" : "登入密码 :" |
| "not\_authentication\_permission" : "未同意指纹使用权限" |
| "notice\_user\_name" : "请输入昵称,7个中英文数字内(必填)" |
| "personal\_info\_withdraw\_password" : "提款密码" |
| "please\_enter\_password" : "请输入提款密码" |
| "please\_enter\_your\_password" : "请输入密码" |
| "registered\_password" : "提款密码" |
| "reset\_password" : "重设密码" |
| "set\_withdraw\_pwd\_first" : "请先至提领页设置您的提款密码" |
| "trans3\_goto\_transhistory" : "前往交易记录" |
| "user\_name" : "用户名称" |
| "vip\_auth" : "VIP权限" |
| "wrong\_password" : "密码错误" |
| "ball\_possession" : "ボールコントロール率" |
| "dialog\_auth\_method\_mail" : "メールアドレス" |
| "dialog\_auth\_method\_mail\_common" : "メールアドレス:" |
| "dialog\_auth\_method\_mobile" : "携帯番号" |
| "dialog\_choose\_auth" : "認証方法" |
| "dialog\_choose\_auth\_common" : "認証方法" |
| "draw\_password" : "引き出しパスワード:" |
| "fingerprint\_auth" : "指紋認証でログイン" |
| "fingerprint\_auth\_not\_ready" : "指紋認証が設定されていません" |
| "fingerprint\_auth\_successful" : "指紋認証成功" |
| "guide\_user\_name" : "マイクマイクマイク…" |
| "inout\_password" : "パスワード入力" |
| "login\_password" : "ログインパスワード：" |
| "not\_authentication\_permission" : "指紋認証の使用権限に同意していません" |
| "notice\_user\_name" : "ニックネームを入力してください。７文字以内英数含む（必須）" |
| "personal\_info\_withdraw\_password" : "出金パスワード" |
| "please\_enter\_password" : "引き出しパスワードを入力してください" |
| "please\_enter\_your\_password" : "パスワードを入力してください" |
| "registered\_password" : "出金パスワード" |
| "reset\_password" : "パスワード再設定" |
| "set\_withdraw\_pwd\_first" : "引き出しページで、引き出しパスワードを設定してください" |
| "trans3\_goto\_transhistory" : "取引記録へ進む" |
| "user\_name" : "ユーザー名" |
| "vip\_auth" : "VIP権限" |
| "wrong\_password" : "パスワード間違い" |
| "auto\_authorization\_description" : "Authorize K7 system auto execute if you don't want to miss any profitable opportunity." |
| "auto\_authorization\_description2" : "Authorize K7 auto execution when placing bets every time." |
| "ball\_possession" : "Possession Rate" |
| "cancel\_authorization" : "Cancel Authorization" |
| "dialog\_auth\_method\_mail" : "Email" |
| "dialog\_auth\_method\_mail\_common" : "Email:" |
| "dialog\_auth\_method\_mobile" : "Mobile" |
| "dialog\_choose\_auth" : "Verification Methods" |
| "dialog\_choose\_auth\_common" : "Verification Methods" |
| "draw\_password" : "Withdraw Password:" |
| "fingerprint\_auth" : "Use fingerprint login" |
| "fingerprint\_auth\_not\_ready" : "Fingerprint recognition setting incomplete" |
| "fingerprint\_auth\_successful" : "Fingerprint recognized" |
| "guide\_user\_name" : "MikeMikeMike..." |
| "inout\_password" : "Enter password" |
| "login\_password" : "Login Password:" |
| "not\_authentication\_permission" : "Disagree with fingerprint access permission." |
| "notice\_user\_name" : "Enter within 7 chars and numbers (\*req)" |
| "personal\_info\_withdraw\_password" : "Withdrawal Password" |
| "please\_enter\_password" : "Please enter withdrawal password." |
| "please\_enter\_your\_password" : "Please enter password" |
| "registered\_password" : "Withdrawal Password" |
| "reset\_password" : "Rest password" |
| "set\_withdraw\_pwd\_first" : "Please go to Withdrawal to set your withdrawal password." |
| "trans3\_goto\_transhistory" : "Go to transactions" |
| "user\_name" : "Username" |
| "vip\_auth" : "VIP Privileges" |
| "wrong\_password" : "Password is incorrect" |
| "ball\_possession" : "볼 점유율" |
| "dialog\_auth\_method\_mail" : "이메일" |
| "dialog\_auth\_method\_mail\_common" : "이메일:" |
| "dialog\_auth\_method\_mobile" : "휴대전화 번호" |
| "dialog\_choose\_auth" : "인증 방식" |
| "dialog\_choose\_auth\_common" : "인증 방식" |
| "draw\_password" : "출금 비밀번호:" |
| "fingerprint\_auth" : "지문으로 로그인" |
| "fingerprint\_auth\_not\_ready" : "지문인식 설정 미완료" |
| "fingerprint\_auth\_successful" : "지문인식 성공" |
| "guide\_user\_name" : "홍길동홍길동…" |
| "inout\_password" : "비밀번호를 입력하세요." |
| "login\_password" : "로그인 비밀번호 :" |
| "not\_authentication\_permission" : "지문 인식 사용 권한을 부여하지 않았습니다." |
| "notice\_user\_name" : "문자, 숫자로 된 닉네임 7자를 입력하세요.(필수)" |
| "personal\_info\_withdraw\_password" : "출금 비밀번호" |
| "please\_enter\_password" : "출금 비밀번호를 입력하세요." |
| "please\_enter\_your\_password" : "비밀번호를 입력하세요." |
| "registered\_password" : "출금 비밀번호" |
| "reset\_password" : "비밀번호 재설정" |
| "set\_withdraw\_pwd\_first" : "먼저 출금 페이지에서 출금 비밀번호를 설정해 주세요." |
| "trans3\_goto\_transhistory" : "거래 기록으로 이동" |
| "user\_name" : "사용자명" |
| "vip\_auth" : "VIP 권한" |
| "wrong\_password" : "비밀번호 오류" |
| "auto\_authorization\_description" : "不想錯過任何一個獲利機會，請授權K7系統自動執行" |
| "auto\_authorization\_description2" : "每次下單時，授權K7系統自動執行" |
| "ball\_possession" : "控球率" |
| "cancel\_authorization" : "取消授權" |
| "dialog\_auth\_method\_mail" : "郵箱" |
| "dialog\_auth\_method\_mail\_common" : "郵箱:" |
| "dialog\_auth\_method\_mobile" : "手機" |
| "dialog\_choose\_auth" : "驗證方式" |
| "dialog\_choose\_auth\_common" : "驗證方式" |
| "draw\_password" : "提領密碼 :" |
| "fingerprint\_auth" : "進行指紋登入" |
| "fingerprint\_auth\_not\_ready" : "指紋辨識未設定完成" |
| "fingerprint\_auth\_successful" : "指紋辨識成功" |
| "guide\_user\_name" : "麥可麥可麥…" |
| "inout\_password" : "輸入密碼" |
| "login\_password" : "登入密碼 :" |
| "not\_authentication\_permission" : "未同意指紋使用權限" |
| "notice\_user\_name" : "請輸入暱稱,7個中英文數字內(必填)" |
| "personal\_info\_withdraw\_password" : "提款密碼" |
| "please\_enter\_password" : "請輸入提款密碼" |
| "please\_enter\_your\_password" : "請輸入密碼" |
| "registered\_password" : "提款密碼" |
| "reset\_password" : "重設密碼" |
| "set\_withdraw\_pwd\_first" : "請先至提領頁設置您的提款密碼" |
| "trans3\_goto\_transhistory" : "前往交易記錄" |
| "user\_name" : "用戶名稱" |
| "vip\_auth" : "VIP權限" |
| "wrong\_password" : "密碼錯誤" |
| "ball\_possession" : "控球率" |
| "dialog\_auth\_method\_mail" : "邮箱" |
| "dialog\_auth\_method\_mail\_common" : "邮箱:" |
| "dialog\_auth\_method\_mobile" : "手机" |
| "dialog\_choose\_auth" : "验证方式" |
| "dialog\_choose\_auth\_common" : "验证方式" |
| "draw\_password" : "提领密码 :" |
| "fingerprint\_auth" : "进行指纹登入" |
| "fingerprint\_auth\_not\_ready" : "指纹辨识未设定完成" |
| "fingerprint\_auth\_successful" : "指纹辨识成功" |
| "guide\_user\_name" : "麦可麦可麦…" |
| "inout\_password" : "输入密码" |
| "login\_password" : "登入密码 :" |
| "not\_authentication\_permission" : "未同意指纹使用权限" |
| "notice\_user\_name" : "请输入昵称,7个中英文数字内(必填)" |
| "personal\_info\_withdraw\_password" : "提款密码" |
| "please\_enter\_password" : "请输入提款密码" |
| "please\_enter\_your\_password" : "请输入密码" |
| "registered\_password" : "提款密码" |
| "reset\_password" : "重设密码" |
| "set\_withdraw\_pwd\_first" : "请先至提领页设置您的提款密码" |
| "trans3\_goto\_transhistory" : "前往交易记录" |
| "user\_name" : "用户名称" |
| "vip\_auth" : "VIP权限" |
| "wrong\_password" : "密码错误" |

## **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.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| 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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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\_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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.POST\_NOTIFICATIONS | 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.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.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 |
| com.lb7be.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 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。**