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

**拉卡拉易分期（ 9.3.1.18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 | 拉卡拉易分期 |
| 版本 | 9.3.1.18 |
| 包名 | com.lakala.android |
| 域名线索 | 15条 |
| URL线索 | 3条 |
| APP图标 |  |
| 分析日期 | 2025年4月3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 | 1745d46911fc0a77d6d3befe4d7926cf.apk |
| 文件大小 | 90.8MB |
| MD5值 | 1745d46911fc0a77d6d3befe4d7926cf |
| SHA1值 | 60bc1c2052d48a00f222ee3ecd0f4be6e0537d0b |
| SHA256值 | f2b8caad1b4ed2cd79b1816813b8c653a578edba9fe7f4a986fa1c28d9c33d28 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 拉卡拉易分期 |
| 包名 | com.lakala.android |
| 主活动Activity | com.lakala.android.activity.EntranceActivity |
| 安卓版本名称 | 9.3.1.18 |
| 安卓版本 | 152 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| metrics-dra.dt.hicloud.com | IP: 94.74.88.100 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.zetetic.net | IP: 99.84.141.117 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| grs.dbankcloud.com | IP: 60.28.193.195 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics2.data.hicloud.com | IP: 80.158.38.48 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| store.hispace.hicloud.com | IP: 49.4.47.241 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| lakala-fintech-firebase.firebaseio.com | IP: 34.120.160.131 所属国家: United States of America 地区: Missouri 城市: Kansas City  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://lakala-fintech-firebase.firebaseio.com  | 摸瓜V1引擎  |
| https://play.google.com/store  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com/app/  | 摸瓜V1引擎  |
| https://play.google.com/store/apps/details?id=  | 摸瓜V1引擎  |
| https://appgallery.cloud.huawei.com  | 摸瓜V1引擎  |
| https://www.zetetic.net/sqlcipher/  | 摸瓜V1引擎  |
| https://www.zetetic.net/sqlcipher/license/  | 摸瓜V1引擎  |
| https://github.com/sqlcipher/android-database-sqlcipher  | 摸瓜V1引擎  |
| https://store.hispace.hicloud.com/hwmarket/api/  | 摸瓜V1引擎  |
| https://metrics1.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics-dra.dt.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics2.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://metrics5.data.hicloud.com:6447  | 摸瓜V2引擎  |
| https://grs.dbankcloud.com  | 摸瓜V2引擎  |
| https://grs.dbankcloud.cn  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://grs.dbankcloud.asia  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **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=beijing, L=beijing, O=lakala, OU=production department, CN=daiqijun 签名算法: rsassa\_pkcs1v15 有效期自: 2012-04-26 05:43:52+00:00 有效期至: 2042-04-19 05:43:52+00:00 发行人: C=CN, ST=beijing, L=beijing, O=lakala, OU=production department, CN=daiqijun 序列号: 0x4f98e098 哈希算法: sha1 md5值: 526648f3d82781b88786d307f505bca3 sha1值: 44f821e79cbec565af6002eb86da424b5bae8e05 sha256值: a170e379137de42003305116b54a63b9e417fd14efa48e04bd5d618ba7347567 sha512值: 5dfc0e5d2a1d8fe8c91266271682bb61c9766d7a57b25feefc7a9dac16da811d9ce191ccb850598a897570d99e0dc21da5fff5a9982cf0935c4416ee9138f7df 公钥算法: rsa 密钥长度: 1024 指纹: 91f037dac0b4e83c0c0d42c75e9bd41bb8e2f60875c73b8bd6ddacf00c9b74cf**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "accountsafe\_managepwd" : "密码管理"  |
| "accountsafe\_wont\_input\_paypwd" : "免输支付密码"  |
| "accountsafe\_wont\_input\_paypwd\_off" : "您已关闭开关，支付时需要输入支付密码"  |
| "accountsafe\_wont\_input\_paypwd\_on" : "您已开启开关，金额≤1000元/笔，无需输入支付密码"  |
| "currently\_password" : "请输入拉卡拉密码"  |
| "firebase\_database\_url" : "https://lakala-fintech-firebase.firebaseio.com"  |
| "google\_api\_key" : "AIzaSyDBPha50ZCHYl7CDfbezXegfILGC9Yo16U"  |
| "google\_crash\_reporting\_api\_key" : "AIzaSyDBPha50ZCHYl7CDfbezXegfILGC9Yo16U"  |
| "input\_bill\_password" : "输入邮箱密码"  |
| "input\_lakala\_password" : "请输入登录密码"  |
| "lakala\_map\_key" : "1557766abd1c0c689304a34236065547a118cbaf1c1b55f2424be28bc9c5c0d7c34ac11981629242"  |
| "library\_android\_database\_sqlcipher\_author" : "Zetetic, LLC"  |
| "library\_android\_database\_sqlcipher\_authorWebsite" : "https://www.zetetic.net/sqlcipher/"  |
| "managepwd\_find\_paypwd" : "找回支付密码"  |
| "managepwd\_input\_login\_password\_again" : "请再次输入新登录密码"  |
| "managepwd\_modify\_gesturepwd" : "修改手势解锁图案"  |
| "managepwd\_modify\_gesturepwd\_decription" : "进入拉卡拉客户端时使用，保护您的账户安全"  |
| "managepwd\_password\_rule" : "登录密码由8-30位英文字母、数字或符号组成；请不要设置与常用软件、网站等相同或相似的密码，并做定期修改"  |
| "managepwd\_set\_login\_password" : "设置登录密码"  |
| "managepwd\_set\_paypwd" : "设置支付密码"  |
| "managepwd\_set\_paypwd\_problem" : "设置密保问题"  |
| "managepwd\_show\_password" : "显示密码"  |
| "pay\_amount\_no\_password" : "付款金额≤%s元/日，无需输入拉卡拉密码"  |
| "plat\_again\_input\_login\_password" : "请再次输入登录密码"  |
| "plat\_authentication\_idNum" : "身份证号"  |
| "plat\_authentication\_idNum\_inputformat\_invalid" : "请输入正确的18位身份证号码"  |
| "plat\_authentication\_name" : "姓名"  |
| "plat\_authentication\_place\_idNum" : "请输入18位身份证号码"  |
| "plat\_authentication\_place\_name" : "请输入您的真实姓名"  |
| "plat\_authentication\_title" : "身份验证"  |
| "plat\_authentication\_verify\_invalid" : "身份验证失败，请重新填写"  |
| "plat\_confim\_login\_lakala\_password" : "确认拉卡拉密码"  |
| "plat\_find\_password" : "找回登录密码"  |
| "plat\_forget\_gestrue\_pwd\_login\_prompt" : "忘记手势密码，需重新登录"  |
| "plat\_forget\_password" : "忘记密码"  |
| "plat\_local\_auth\_faceid" : "点击进行面容解锁"  |
| "plat\_local\_auth\_touchid" : "点击进行指纹解锁"  |
| "plat\_login\_lakala\_password" : "拉卡拉密码"  |
| "plat\_login\_password" : "登录密码"  |
| "plat\_password" : "密码"  |
| "plat\_password\_security\_find\_pay\_pwd\_title" : "找回支付密码"  |
| "plat\_please\_again\_input\_login\_password" : "请再次输入以确认"  |
| "plat\_please\_confim\_login\_password" : "请再次输入拉卡拉密码"  |
| "plat\_please\_input\_login\_password" : "输入登录密码"  |
| "plat\_plese\_input\_your\_password" : "请输入您的密码"  |
| "plat\_reset\_gesture\_password" : "重新绘制图案"  |
| "plat\_reset\_login\_password" : "重置登录密码"  |
| "plat\_reset\_pwd\_success\_prompt" : "设置成功，请使用新密码登录"  |
| "plat\_session\_expired" : "登录已过期,请重新登录"  |
| "plat\_set\_gesture\_password" : "设置手势密码"  |
| "plat\_set\_login\_lakala\_password" : "设置登录密码"  |
| "plat\_set\_pay\_input\_password" : "请输入当前支付密码"  |
| "plat\_set\_pay\_password" : "设置拉卡拉支付密码"  |
| "plat\_show\_password" : "显示密码"  |
| "plat\_swipe\_input\_password" : "请输入密码"  |
| "plat\_to\_set\_pay\_password" : "去设置"  |
| "plat\_verify\_password" : "验证密码"  |
| "please\_again\_input\_specially\_password" : "请重新输入独立密码"  |
| "please\_input\_mail\_pwd" : "请输入邮箱密码"  |
| "please\_input\_specially\_password" : "请输入独立密码"  |
| "swiper\_card\_password" : "输入银行卡密码"  |
| "weibo\_oauth\_regiseter" : "应用授权"  |

## **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.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.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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_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.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.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.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\_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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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。  |
| android.permission.SYSTEM\_OVERLAY\_WINDOW | 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。 |
| 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.USE\_BIOMETRIC | 正常 |  | 允许应用使用设备支持的生物识别模式。 |
| com.lakala.android.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.lakala.android.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.lakala.android.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.lakala.android.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BLUETOOTH\_PRIVILEGED | 系统需要 |  | 允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或消息访问。这不适用于第三方应用程序 |
| 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 |
| com.lakala.android.permission.PUSH\_PROVIDER | 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 |
| android.permission.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.INTERACT\_ACROSS\_USERS\_FULL | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| 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.lakala.android.activity.EntranceActivity | **Schemes**: koala://, **Hosts:** client,  |
| com.lakala.android.activity.common.CashierTransitActivity | **Schemes**: koala://, **Hosts:** pay,  |
| com.mob.tools.MobUIShell | **Schemes**: tencent100830840://,  |

**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。**