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

**分期乐（ 1.0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 | 分期乐 |
| 版本 | 1.0 |
| 包名 |  |
| 域名线索 | 33条 |
| URL线索 | 13条 |
| APP图标 |  |
| 分析日期 | 2025年6月26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.fenqile.fenqile\_691.apk |
| 文件大小 | 122.3MB |
| MD5值 | 51e51f84dfa92b9f29cdd4b271bc5f50 |
| SHA1值 | b02118832b2dcb9f2ace91bca55cb8fc38c6728a |
| SHA256值 | 28fdbca273b76f254227bb93e5d693775a639b80a8d6889f56000ef5847a9f77 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 分期乐 |
| 包名 |  |
| 主活动Activity | [] |
| 安卓版本名称 | 1.0 |
| 安卓版本 | [] |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| grs.dbankcloud.eu | 没有服务器地理信息.  |
| data-drcn.push.dbankcloud.com | IP: 49.4.40.58 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| metrics1.data.hicloud.com | IP: 111.202.16.252 所属国家: China 地区: Beijing 城市: Beijing  |
| www.winimage.com | IP: 205.251.81.217 所属国家: United States of America 地区: New Jersey 城市: Parsippany  |
| unpkg.com | IP: 104.17.245.203 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics5.dt.dbankcloud.ru | 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  |
| t.captcha.qq.com | IP: 60.29.242.237 所属国家: China 地区: Tianjin 城市: Tianjin  |
| captcha.gtimg.com | IP: 119.167.147.251 所属国家: China 地区: Shandong 城市: Qingdao  |
| www.intel.com | IP: 23.201.252.235 所属国家: Germany 地区: Hessen 城市: Frankfurt am Main  |
| data-dra.push.dbankcloud.com | IP: 119.8.163.189 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  |
| aq.qq.com | IP: 140.207.58.65 所属国家: China 地区: Shanghai 城市: Shanghai  |
| grs.platform.dbankcloud.ru | 没有服务器地理信息.  |
| grs.dbankcloud.cn | IP: 121.36.116.8 所属国家: China 地区: Beijing 城市: Beijing  |
| opensource.org | IP: 172.67.197.41 所属国家: United States of America 地区: California 城市: San Francisco  |
| render.alipay.com | IP: 101.72.221.202 所属国家: China 地区: Hebei 城市: Langfang  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| stream.feedcoopapi.com | IP: 221.194.131.54 所属国家: China 地区: Beijing 城市: Beijing  |
| play.google.com | IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan  |
| fm.fenqile.com | IP: 119.29.42.120 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.ietf.org | IP: 104.16.44.99 所属国家: United States of America 地区: California 城市: San Francisco  |
| data-dre.push.dbankcloud.com | IP: 80.158.49.244 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| grs.dbankcloud.asia | IP: 49.4.40.185 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.webrtc.org | IP: 142.251.33.110 所属国家: Canada 地区: Ontario 城市: Toronto  |
| www.w3.org | IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| metrics2.data.hicloud.com | IP: 80.158.2.190 所属国家: Germany 地区: Schleswig-Holstein 城市: Kiel  |
| metrics5.data.hicloud.com | IP: 159.138.203.215 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| www.mob.com | IP: 45.113.201.237 所属国家: China 地区: Jiangsu 城市: Yangzhou  |
| appgallery.cloud.huawei.com | IP: 49.4.35.16 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| openfql.oa.fenqile.com | IP: 119.29.157.20 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| data-drru.push.dbankcloud.com | IP: 159.138.202.31 所属国家: Russian Federation 地区: Sverdlovskaya oblast' 城市: Yekaterinburg  |
| dc.fenqile.com | IP: 159.75.145.28 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/yuyan/180020010001208736/aliyunFacewelcome.html  | 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  |
| http://www.mob.com  | 摸瓜V1引擎  |
| https://stream.feedcoopapi.com/user/event/log/video/v1/  | 摸瓜V2引擎  |
| https://aq.qq.com/cn2/manage/mbtoken/cap\_monitor?  | 摸瓜V2引擎  |
| https://t.captcha.qq.com  | 摸瓜V2引擎  |
| https://captcha.gtimg.com/1  | 摸瓜V2引擎  |
| https://fm.fenqile.com/route0014  | 摸瓜V2引擎  |
| https://openfql.oa.fenqile.com/oa/mobile  | 摸瓜V2引擎  |
| https://data-drcn.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dra.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-dre.push.dbankcloud.com  | 摸瓜V2引擎  |
| https://data-drru.push.dbankcloud.com  | 摸瓜V2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://metrics5.dt.dbankcloud.ru: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.asia  | 摸瓜V2引擎  |
| https://grs.platform.dbankcloud.ru  | 摸瓜V2引擎  |
| https://grs.dbankcloud.eu  | 摸瓜V2引擎  |
| https://unpkg.com/pdfjs-dist@1.9.426/cmaps/';  | 摸瓜V2引擎  |
| https://github.com/Tencent/vConsole)  | 摸瓜V2引擎  |
| http://opensource.org/licenses/MIT  | 摸瓜V2引擎  |
| https://github.com/Tencent/vConsole  | 摸瓜V2引擎  |
| https://github.com/Tencent/vConsole.git  | 摸瓜V2引擎  |
| https://dc.fenqile.com/route0031/dataCollect/uploadWebDataSingleReport.json  | 摸瓜V2引擎  |
| https://dc.fenqile.com/route0031/reportStrategy/queryWebStrategy.json  | 摸瓜V2引擎  |
| http://www.winimage.com/zLibDll  | lib/armeabi-v7a/libVolcBaseLog.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay  | lib/armeabi-v7a/libbyterts.so  |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-01  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-02  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/meta-data-03  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/decoding-timestamp  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-composition-time  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-type  | lib/armeabi-v7a/libbyterts.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/order-in-stream  | lib/armeabi-v7a/libbyterts.so  |
| http://www.intel.com/software/products/support/.  | lib/armeabi-v7a/libface\_detect.so  |

### **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: CN=denny 签名算法: rsassa\_pkcs1v15 有效期自: 2014-07-02 03:10:17+00:00 有效期至: 2039-06-26 03:10:17+00:00 发行人: CN=denny 序列号: 0x25090221 哈希算法: sha256 md5值: 94378bbc5423a6075f69014f5b94467a sha1值: 88f15effef8717bebefa7a9317acd5738e6f7840 sha256值: 864d152aeb9c303afdac0fbd8885087364a463db92dbf85a31c8cb257a8f5e5e sha512值: 5b3912d6bf97572a95a0ed2c17028b614b01808036123885538dd893fc3b952d41c8bb9d908b65b4ee30bbf3bfe4bbe66af2178b4c85a4daca7e5cfced6b1f8c 公钥算法: rsa 密钥长度: 2048 指纹: fb8a90e45a470a54d91c272af19acd2432011783f1419d995d415d2acfcb11fa**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "gt\_one\_login\_auth\_btn" : "一键登录"  |
| "image\_picker\_provider\_authority\_suffix" : ".imagepicker.provider"  |
| "login\_account\_pwd\_login" : "账号密码登录"  |
| "login\_set\_deal\_password" : "设置交易密码"  |
| "login\_set\_login\_password" : "设置登录密码"  |
| "secret\_key\_name" : "biometric\_fenqile\_encryption\_key"  |
| "ssdk\_instapaper\_pwd" : "密码"  |
| "ssdk\_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**

## **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。**