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

**樱桃（ 3.2.6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 | 樱桃 |
| 版本 | 3.2.6 |
| 包名 | banfy.o1lxx.a43hj |
| 域名线索 | 7条 |
| URL线索 | 4条 |
| APP图标 |  |
| 分析日期 | 2025年7月9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 | yingtao.apk |
| 文件大小 | 58.85MB |
| MD5值 | e75207eae39a4dc0abe0044a9ac99a46 |
| SHA1值 | c36b130ded8fc59d4f4f43e7fa3c750e3e6211c7 |
| SHA256值 | 59cf6e3a16985879464709093d9c68a176cec97952fad31a8b136d927fbab443 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 樱桃 |
| 包名 | banfy.o1lxx.a43hj |
| 主活动Activity | com.yunbao.phonelive.activity.LauncherActivity |
| 安卓版本名称 | 3.2.6 |
| 安卓版本 | 900036 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| 139.224.238.21 | IP: 139.224.238.21 所属国家: China 地区: Shanghai 城市: Shanghai  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| confluence.agoralab.co | IP: 123.126.74.241 所属国家: China 地区: Beijing 城市: Beijing  |
| www.webrtc.org | IP: 142.250.69.174 所属国家: United States of America 地区: California 城市: Mountain View  |
| api.hcharts.cn | IP: 47.98.237.147 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.highcharts.com | IP: 104.18.9.9 所属国家: United States of America 地区: California 城市: San Francisco  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/vinc3m1  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView  | 摸瓜V1引擎  |
| https://github.com/vinc3m1/RoundedImageView.git  | 摸瓜V1引擎  |
| https://api.hcharts.cn/highcharts  | 摸瓜V2引擎  |
| https://www.highcharts.com?credits  | 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  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1161004477  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| https://confluence.agoralab.co/pages/viewpage.action?pageId=1035862602  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://s?  | lib/arm64-v8a/libagora-rtc-sdk.so  |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor  | 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**

## **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=adminggi\_uq, ST=adminggi\_uq, L=adminggi\_uq, O=adminggi\_uq, OU=adminggi\_uq, CN=adminggi\_uq 签名算法: rsassa\_pkcs1v15 有效期自: 2024-11-09 11:45:21+00:00 有效期至: 2124-10-16 11:45:21+00:00 发行人: C=adminggi\_uq, ST=adminggi\_uq, L=adminggi\_uq, O=adminggi\_uq, OU=adminggi\_uq, CN=adminggi\_uq 序列号: 0x40a3cfe0 哈希算法: sha256 md5值: 4d6f7da5309842c5b91ed17bab41b941 sha1值: 4a0b410245ec5edb35c7b5bf908b26f560621971 sha256值: 771d8e7299a1dd796d17a9babdd8888abff889673d1e99bd9cf69752cc14904f sha512值: a25c4db078efc955af1cb7403cb9e23b34fcddb3f41de2b17805ccdf8729ea38574da25cf9a7427c8eba2c5ce481e79a99831bf22aaff85879ace1edca6a0d45 公钥算法: rsa 密钥长度: 1024 指纹: 57f4a5f1fc152e939c6f78d52d7511acc4e7fadd13e27a8350f2d13008c42bc1**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "cash\_input\_bank\_user\_name" : "请输入持卡人姓名"  |
| "emotion\_status\_secret" : "保密"  |
| "enter\_withdraw\_pwd" : "请输入提现密码"  |
| "find\_pwd" : "找回密码"  |
| "find\_pwd\_find" : "立即找回"  |
| "find\_pwd\_forget" : "忘记密码"  |
| "follow\_author" : "关注主播"  |
| "input\_payment\_password" : "请输入支付密码(6位纯数字)"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "live\_input\_password" : "请输入房间密码"  |
| "live\_set\_pwd" : "请设置房间密码"  |
| "live\_type\_pwd" : "密码房间"  |
| "login\_auth\_cancle" : "授权取消"  |
| "login\_auth\_failure" : "授权失败"  |
| "login\_auth\_ing" : "正在授权登录"  |
| "login\_auth\_success" : "登录成功"  |
| "login\_forget\_pwd" : "忘记密码"  |
| "login\_input\_pwd" : "请输入密码"  |
| "main\_live\_type\_pwd" : "密码"  |
| "mobile\_authentication" : "手机认证"  |
| "modify\_pwd" : "重置密码"  |
| "payment\_password" : "支付密码"  |
| "phone\_auth" : "手机绑定"  |
| "promotion\_user" : "用户"  |
| "reg\_input\_pwd\_1" : "请填写密码"  |
| "reg\_input\_pwd\_2" : "请确认密码"  |
| "reg\_input\_pwd\_3" : "邀请码(选填)"  |
| "withdraw\_pwd\_str" : "提现密码"  |

## **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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.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.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.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\_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.NETWORK\_PROVIDER | 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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 |
| 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.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.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.REORDER\_TASKS | 正常 | 重新排序正在运行的应用程序 | 允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前 |
| 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.MANAGE\_ACCOUNTS | 危险 | 管理帐户列表 | 允许应用程序执行添加和删除帐户以及删除其密码等操作 |
| android.permission.RECEIVE\_USER\_PRESENT | 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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_PRIVILEGED\_PHONE\_STATE | 未知 | Unknown permission | Unknown permission from android reference |
| 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**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.yunbao.common.arouter.SchemeFilterActivity | **Schemes**: guming://, **Hosts:** com.guming,  |

**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。**