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

**水云涧（ 2.0.6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 | 水云涧 |
| 版本 | 2.0.6 |
| 包名 | com.shuiyunjiannew.chat |
| 域名线索 | 4条 |
| URL线索 | 7条 |
| APP图标 |  |
| 分析日期 | 2025年8月10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 | base.apk |
| 文件大小 | 38.46MB |
| MD5值 | 9bc3e3f30d8ccbe780310e2523570f47 |
| SHA1值 | 1dddeceb360f005b1fc3a7a076cc3c626c5e20d0 |
| SHA256值 | 8958b6afff344e412988b23bb9886edc2d5e42e1a01a762f9b4160e8b5ab97d3 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 水云涧 |
| 包名 | com.shuiyunjiannew.chat |
| 主活动Activity | com.shuiyunjiannew.chat.activity.SplashActivity |
| 安卓版本名称 | 2.0.6 |
| 安卓版本 | 11 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| appcashier256.95516.com | IP: 124.166.227.171 所属国家: China 地区: Shanxi 城市: Taiyuan  |
| argus.agoralab.co | IP: 116.140.34.226 所属国家: China 地区: Liaoning 城市: Shenyang  |
| appcashier.test.95516.com | IP: 180.95.171.99 所属国家: China 地区: Gansu 城市: Jinchang  |
| www.openssl.org | IP: 34.49.79.89 所属国家: United States of America 地区: California 城市: Mountain View  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.openssl.org/docs/faq.html  | lib/armeabi-v7a/libqcOpenSSL.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libnative.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libuptsmaddonmi.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libuptsmaddon.so  |
| http://argus.agoralab.co/vosdk/public/report?speaker=%u&listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk-jni.so  |
| http://argus.agoralab.co/vosdk/public/report?listener=%u&venderID=%s&channelName=%s  | lib/armeabi-v7a/libagora-rtc-sdk-jni.so  |
| https://appcashier256.95516.com/gateway/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/conf  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/conf  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/hft  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/hft  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/app/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier256.95516.com/app/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| https://appcashier.test.95516.com/gateway/mobile/json  | lib/armeabi-v7a/libentryexpro.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libagora-crypto.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |
| jrs@cs.berkeley  | lib/armeabi-v7a/libnama.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=CN, CN=shuiyunjian 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-12 15:09:37+00:00 有效期至: 2050-05-13 15:09:37+00:00 发行人: C=CN, CN=shuiyunjian 序列号: 0x594d0000000000f52ec1 哈希算法: sha256 md5值: 43b32a9ceeaa065be318b27533664c99 sha1值: 212e3389de29cc349d890e1374c06baff2443eef sha256值: 1b235da4ef1d0f123b03e54075351e7c42440bb960dfd48600455561b2155352 sha512值: b9a9888eb08ed0601cf65ec831930a3bac457d787694083977c3ef2f0b9881f1d429befaec277b0e4104dfeb2b7c48159c200c016da9fdc630b6857b57dc3632 公钥算法: rsa 密钥长度: 2048 指纹: f4e7a7b38b6912c8679b55ee059d932dc216a426d35faab45126c32904d4e4ac**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "account\_password" : "账号密码登录"  |
| "active\_user" : "活跃用户:"  |
| "chat\_user" : "聊友:"  |
| "forget\_password" : "忘记密码?"  |
| "input\_password" : "输入密码"  |
| "need\_independent\_password" : "启动未成年模式,需要设置独立密码"  |
| "online\_user" : "当前在线用户: 5562次"  |
| "password" : "密 码:"  |
| "phone\_private" : "私密(不公开)"  |
| "please\_input\_active\_user" : "请输入您的活跃用户"  |
| "please\_input\_long\_password" : "密码长度不够"  |
| "please\_input\_password" : "请输入密码"  |
| "private\_agree" : "《隐私政策》"  |
| "private\_chat\_switch" : "私信聊天"  |
| "private\_detail" : "隐私政策"  |
| "private\_image" : "私密照片"  |
| "private\_video" : "私密视频"  |
| "swtich\_off\_alert\_private" : "关闭后你将收不到私聊消息"  |
| "token\_invalid" : "登录失效，请重新登录"  |
| "verify\_password" : "验证密码"  |
| "wrong\_password" : "密码不正确,请重新输入"  |

## **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.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.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\_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\_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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| com.shuiyunjiannew.chat.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| 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\_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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.USE\_FULL\_SCREEN\_INTENT | 正常 |  | 针对想要使用通知全屏意图的 Build.VERSION\_CODES.Q 的应用程序是必需的 |
| 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。 |
| 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 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent101://,  |

**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。**