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

**98娱乐（ 3.0.53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 | 98娱乐 |
| 版本 | 3.0.53 |
| 包名 | com.dsn.platform98 |
| 域名线索 | 10条 |
| URL线索 | 14条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | 98cp.apk |
| 文件大小 | 103.18MB |
| MD5值 | 38868f8a080cce414c56b5ee2793a35c |
| SHA1值 | c8e248ce536bb9694b8ff3494da5300555c2a02d |
| SHA256值 | 6190aba93eacc904a843f8b66a690cccd6a27a9c2ff740d7b0678d4a9549e07c |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 98娱乐 |
| 包名 | com.dsn.platform98 |
| 主活动Activity | com.wind2cashapp.MainActivity |
| 安卓版本名称 | 3.0.53 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.facebook.com | IP: 104.244.46.57 所属国家: United States of America 地区: California 城市: San Francisco  |
| ce3e75d5.jpush.cn | IP: 120.233.118.242 所属国家: China 地区: Guangdong 城市: Shenzhen  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| codepush.appcenter.ms | IP: 52.232.227.249 所属国家: United States of America 地区: Virginia 城市: Boydton  |
| pinterest.com | IP: 103.252.115.59 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| docs.swmansion.com | IP: 172.67.142.188 所属国家: United States of America 地区: California 城市: San Francisco  |
| dnsrepo-pub.alibaba.com | IP: 203.119.174.99 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| plus.google.com | IP: 66.220.149.18 所属国家: United States of America 地区: California 城市: Menlo Park  |
| twitter.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| play.google.com | IP: 46.82.174.69 所属国家: Germany 地区: Niedersachsen 城市: Braunschweig  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://ce3e75d5.jpush.cn/wi/cjc4sa  | cn/jiguang/au/c.java  |
| https://ce3e75d5.jpush.cn/wi/d8n3hj  | cn/jiguang/au/c.java  |
| https://www.facebook.com/sharer/sharer.php?u=  | cl/json/social/FacebookPagesManagerShare.java  |
| https://pinterest.com/pin/create/button/?url=  | cl/json/social/PinterestShare.java  |
| https://twitter.com/intent/tweet?text=  | cl/json/social/TwitterShare.java  |
| https://www.facebook.com/sharer/sharer.php?u=  | cl/json/social/FacebookShare.java  |
| https://plus.google.com/share?url=  | cl/json/social/GooglePlusShare.java  |
| https://play.google.com/store/apps/details?id=com.instagram.android  | cl/json/social/InstagramShare.java  |
| https://play.google.com/store/apps/details?id=com.instagram.android  | cl/json/social/InstagramStoriesShare.java  |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermData  | com/alibaba/pdns/g.java  |
| https://dnsrepo-pub.alibaba.com/api/internet/putTermStatusData  | com/alibaba/pdns/g.java  |
| http://support.newrelic.com.  | com/newrelic/agent/android/NewRelic.java  |
| https://codepush.appcenter.ms/  | com/microsoft/codepush/react/CodePush.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenStackFragment.java  |
| https://github.com/software-mansion/react-native-screens/issues/17  | com/swmansion/rnscreens/ScreenFragment.java  |
| https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot  | com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java  |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15569251296  | net/time4j/calendar/VietnameseCalendar.java  |
| 15569251296  | net/time4j/calendar/ChineseCalendar.java  |
| 15569251296  | net/time4j/calendar/KoreanCalendar.java  |
| 14403429586  | net/time4j/calendar/hindu/HinduVariant.java  |
| 15040511099  | net/time4j/tz/model/SPX.java  |
| 18067104000  | net/time4j/tz/model/SPX.java  |

## **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=SG, ST=Tanjong Pagar, L=Tanjong Pagar, O=Orion Consultancy, OU=Mobile Development, CN=Avery Choke 签名算法: rsassa\_pkcs1v15 有效期自: 2018-02-26 09:04:40+00:00 有效期至: 2043-02-20 09:04:40+00:00 发行人: C=SG, ST=Tanjong Pagar, L=Tanjong Pagar, O=Orion Consultancy, OU=Mobile Development, CN=Avery Choke 序列号: 0x7f139e2d 哈希算法: sha256 md5值: e4b29352d272f9084a9958a9a6bd7d3a sha1值: e9e5cae2f41bfd1c37d5d577072fb60fc3cb3a78 sha256值: d2cb544f4ee4d64be057ddd1af177f968b5dfdeed82603a59e5bf4cc79be9186 sha512值: 52cbf40b90b4ce76f8f5e97c13cfa83456443047623a6e08694b9f5bdb6547cd20f071fe40549aec76f90d105faeeb4a52bb7dfd8b2cadecb8cb044056eef6df 公钥算法: rsa 密钥长度: 2048 指纹: 5bc737341ba3959ccf060b735717699a70cbb5807d9fa5e5b1f33ac438b0b93a**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CodePushDeploymentKey" : ""  |

## **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.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.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.DOWNLOAD\_WITHOUT\_NOTIFICATION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |
| com.dsn.platform98.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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\_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.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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.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\_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\_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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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 |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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 |

## **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。**