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

**株洲停车（ V1.0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 | 株洲停车 |
| 版本 | V1.0 |
| 包名 | com.zzgysygs.zztc |
| 域名线索 | 0条 |
| URL线索 | 0条 |
| APP图标 |  |
| 分析日期 | 2025年2月23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 | zhuzhoutingche (1).apk |
| 文件大小 | 10.18MB |
| MD5值 | 566efa36f393f79e5ac4db3c7e228a87 |
| SHA1值 | 854bc483b36c95fc7ec65b0c1be273057b7eb983 |
| SHA256值 | 8c79fe9b74e2ffbc8b206bd0986300da2a53b96610439895d6b7d0298d266b09 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 株洲停车 |
| 包名 | com.zzgysygs.zztc |
| 主活动Activity | com.innotek.goodparking.activity.SplashActivity |
| 安卓版本名称 | V1.0 |
| 安卓版本 | 18 |

## **4. 线索情况**

### **4.1 域名线索**

### **4.2 URL线索**

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| 6h@fo.lwft w9oi\_2nhels4u@dlilycclglhl.5jlcg\_bqh yay@y.u5vcghyy  | lib/armeabi/libiconv.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: False v3 签名: False 找到 1 个唯一证书 主题: ST=浙江, L=杭州, O=浙江创泰科技有限公司 签名算法: rsassa\_pkcs1v15 有效期自: 2015-02-06 03:03:57+00:00 有效期至: 2114-01-13 03:03:57+00:00 发行人: ST=浙江, L=杭州, O=浙江创泰科技有限公司 序列号: 0x39f4c20d 哈希算法: sha256 md5值: afd7299bae15518ac924603267a33445 sha1值: 9094a5bedde253d065b6f6981fb2cdd3d39b4801 sha256值: f0dd210685ebb4ec7e148918071a66e5f4e3bf9945f034bf41000b9e1da7b434 sha512值: 4906125090f1abcf87bc5a6c559c7b1cc1fde52c6fb5b9f52bd13e2bba6c5c63446750702a43d8e47622054fb04860697c7a01d8783f5ae2a091bd6f3671ebb5**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "preference\_key\_tts\_speed" : "50"  |
| "preference\_key\_tts\_volume" : "tts\_volume"  |
| "preference\_key\_tts\_pitch" : "tts\_pitch"  |
| "cmbkb\_publickey" : "aP28KufJh9SXSNjAa/8uUmY0xWKImkTaQVcQACeXGK44QOLAbYo4F+2TQ2O010DHwMAPAq8OeELxHK6BTAaxVUao4jOiCFSqpnoZ0MH4U58kgq9RoAkcSskUAVEtJT16w8UoguX6VTYjJ/EWOwaRNcxb4taIPi6S8AnwTXfniIeuzo1LsMOLlACY3+PAQJDYO4/47Wf/cTDB9Fqu6J7ab9+EueLsBrWR0uQ/h+ANM+VE19s7UikisumSd06fIg8aOFORj/1zjmWMi8u+7FESFYywROQVcd+v8HCJoKnVdJQaAd3Nu4cVx+34PE3K46UqyTi36JkvGX6ZZDK/ImRukQ=="  |
| "tip\_input\_pwd" : "请输入新密码"  |
| "tip\_pwd\_length\_verify" : "新密码长度有误，请确保密码长度为6-16位"  |
| "tip\_rest\_pwd\_success" : "重置密码成功"  |
| "tip\_check\_pwd" : "请检查登录密码！"  |
| "tip\_login\_pwd" : "请输入密码"  |
| "tip\_checkPwd\_num" : "请检查密码位数"  |
| "tip\_twopwd\_notconsistent" : "两次输入的密码不一致，请重新输入"  |
| "tip\_ipnut\_searchKey" : "请输入搜索关键字"  |
| "set\_payment\_pwd" : "设置支付密码"  |
| "modify\_payment\_pwd" : "修改支付密码"  |
| "please\_input\_paymentpwd" : "请输入支付密码"  |
| "please\_original\_paymentpwd" : "请输入原支付密码"  |
| "please\_setpwd\_success" : "密码设置成功"  |

## **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.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.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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\_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.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.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.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.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。 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ\_SETTINGS | 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 |
| android.permission.RECEIVE\_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| 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.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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.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.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。  |
| getui.permission.GetuiService.com.zzgysygs.zztc | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.SET\_DEBUG\_APP | 危险 | 启用应用程序调试 | 允许一个应用程序打开另一个应用程序的调试。恶意应用程序可以使用它来杀死其他应用程序 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.USE\_CREDENTIALS | 危险 | 使用帐户的身份验证凭据 | 允许应用程序请求身份验证令牌 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1104924935://,  |

**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。**