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

**My Car（ V.23.04.25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 | My Car |
| 版本 | V.23.04.25 |
| 包名 | MyCar.apk |
| 域名线索 | 4条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年7月2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 | MyCar.apk |
| 文件大小 | 4.65MB |
| MD5值 | 1fb2cf3bcc8d05e76924125e2014ed9f |
| SHA1值 | 260ff8674a33c9298f2d747e19c9edd2b7f29afb |
| SHA256值 | db07f4ae4eaa192cf684a08697b526d95d9070d6b3661cb5ad74768cfad8e94a |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | My Car |
| 包名 | MyCar.apk |
| 主活动Activity | [] |
| 安卓版本名称 | V.23.04.25 |
| 安卓版本 | 230425 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.nwdcloud.com | IP: 27.185.233.62 所属国家: China 地区: Hebei 城市: Shijiazhuang  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| baidu.com | IP: 110.242.68.66 所属国家: China 地区: Hebei 城市: Baoding  |
| www.nowada.com | IP: 183.62.67.74 所属国家: China 地区: Guangdong 城市: Shenzhen  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| http://www.nwdcloud.com/apis/canapp  | com/nwd/mycar/manager/OkGoManager.java  |
| http://www.nwdcloud.com/cancloud2/getCanUpdateVersionList?data=  | com/nwd/mycar/manager/OkGoManager.java  |
| http://www.nwdcloud.com/cancloud2/getCanUpdateUrl?data=  | com/nwd/mycar/manager/OkGoManager.java  |
| https://baidu.com/  | com/nwd/mycar/thread/NetworkThread.java  |
| http://www.nowada.com:8100/ckcloud/interfaces/can  | com/nwd/mycar/define/NetConst.java  |
| http://www.nwdcloud.com/apis/  | com/nwd/sdk/netapp/SDKNetConf.java  |
| http://www.nowada.com:8166/apis/app360  | com/nwd/sdk/netapp/SDKNetapp.java  |
| http://www.nwdcloud.com/apis/app360  | com/nwd/sdk/netapp/SDKNetapp.java  |
| http://www.nwdcloud.com/ckcloud/interfaces/dsp  | com/nwd/sdk/netapp/SDKNetapp.java  |
| http://www.nwdcloud.com/apis/dspcarkit  | com/nwd/sdk/netapp/SDKNetapp.java  |

### **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: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 签名算法: rsassa\_pkcs1v15 有效期自: 2013-12-03 01:47:50+00:00 有效期至: 2041-04-20 01:47:50+00:00 发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com 序列号: 0xc8e2fec5ee08adf5 哈希算法: sha1 md5值: ffa65da6f2b563fa05ed006256e84564 sha1值: b6a1684c74d7899da8954db8957821f920c66a46 sha256值: 715eb4d74f69a426a5cc8e57c6d8b528cc4967d0b3502005aaaf23aaeb507590 sha512值: 815cb26331dab20a6bbb25deb219f5dd52d450a3b613c66fb9e70d46b33205709d6f296fcf8d704409f24e85acef320d66710d0028461fe98cd9eed233c4ea9e 公钥算法: rsa 密钥长度: 2048 指纹: 5a1c919729bc0bb6db0737a3e56817bfad5849bfaaf74ef89d20a7c2a643959e**

## **6. 硬编码敏感信息**

## **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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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\_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.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.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.READ\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.WRITE\_MEDIA\_STORAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| android.permission.ACCESS\_CACHE\_FILESYSTEM | 系统需要 | 访问缓存文件系统 | 允许应用程序读取和写入缓存文件系统 |
| android.permission.MASTER\_CLEAR | 系统需要 | 将系统重置为出厂默认值 | 允许应用程序将系统完全重置为其出厂设置,擦除所有数据,配置和已安装的应用程序 |
| android.permission.DEVICE\_POWER | 合法 | 打开或关闭手机 | 允许应用程序打开或关闭手机 |
| android.permission.REBOOT | 系统需要 | 强制手机重启 | 允许应用强制手机重启 |
| android.permission.RECOVERY | 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。 |

## **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。**