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

**卡色（ 1.1.4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 | 卡色 |
| 版本 | 1.1.4 |
| 包名 | com.kszs.lw |
| 域名线索 | 20条 |
| URL线索 | 18条 |
| APP图标 |  |
| 分析日期 | 2025年7月16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(1).apk |
| 文件大小 | 15.74MB |
| MD5值 | c81a656aefbf3ebcc0c47ceb55f9f8ff |
| SHA1值 | 7e243d28ef4acc7cdf7a501b9b61d80323486047 |
| SHA256值 | a7dd1f7c3b8263468a476912fdc12eb488d43023d5d85fe71e5949ba7f44bae4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 卡色 |
| 包名 | com.kszs.lw |
| 主活动Activity | com.android.ui.SplashActivity |
| 安卓版本名称 | 1.1.4 |
| 安卓版本 | 1000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| tbsrecovery.imtt.qq.com | IP: 60.28.215.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| xmlpull.org | IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| i.tddmp.com | IP: 116.196.71.30 所属国家: China 地区: Beijing 城市: Beijing  |
| me.xdrig.com | IP: 180.184.82.170 所属国家: China 地区: Beijing 城市: Beijing  |
| av1.xdrig.com | IP: 0.0.0.0 所属国家: - 地区: - 城市: -  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| javax.xml.xmlconstants | 没有服务器地理信息.  |
| cloud.xdrig.com | IP: 116.198.14.26 所属国家: China 地区: Beijing 城市: Beijing  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| 127.0.0.1 | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.slf4j.org | IP: 159.100.250.151 所属国家: Switzerland 地区: Zurich 城市: Zurich  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/evernote/android-job/wiki/FAQ  | com/evernote/android/job/l0ollol1loo0l0ll.java  |
| https://github.com/rmtheis/tess-two/issues/239  | com/googlecode/tesseract/android/TessBaseAPI.java  |
| https://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| https://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://pms.mb.qq.com/rsp204  | com/tencent/smtt/sdk/l.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/ui/dialog/d.java  |
| https://mdc.html5.qq.com/d/directdown.jsp?channel\_id=50079  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/stat/MttLoader.java  |
| https://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/m.java  |
| https://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/m.java  |
| https://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/m.java  |
| https://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/m.java  |
| https://tbsrecovery.imtt.qq.com/getconfig  | com/tencent/smtt/utils/m.java  |
| https://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| https://cloud.xdrig.com/configcloud/rest/sdk/gdprCheck  | com/tendcloud/tenddata/aa.java  |
| https://av1.xdrig.com/u/a/v1  | com/tendcloud/tenddata/aa.java  |
| https://cloud.xdrig.com/configcloud/rest/sdk/match  | com/tendcloud/tenddata/aa.java  |
| https://me.xdrig.com  | com/tendcloud/tenddata/a.java  |
| http://i.tddmp.com/a/  | com/tendcloud/tenddata/ca.java  |
| http://xmlpull.org/v1/doc/features.html  | l0l0ll0lo/ll000l/lo1oll101.java  |
| http://xmlpull.org/v1/doc/features.html  | l0l0ll0lo/ll000l/ol01lo0ol.java  |
| http://www.slf4j.org/codes.html  | l0l0ll0lo/ll000l/cr.java  |
| http://127.0.0.1:%s/cmd  | l0l0ll0lo/ll000l/h56.java  |
| http://127.0.0.1:%s/cmd2  | l0l0ll0lo/ll000l/h56.java  |
| http://127.0.0.1:%s/ping  | l0l0ll0lo/ll000l/h56.java  |
| https://github.com/TooTallNate/Java-WebSocket/wiki/Lost-connection-detection  | org/java\_websocket/AbstractWebSocket.java  |
| http://127.0.0.1  | org/mozilla/javascript/tools/debugger/Dim.java  |
| http://javax.xml.XMLConstants/feature/secure-processing  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://apache.org/xml/features/disallow-doctype-decl  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://apache.org/xml/features/nonvalidating/load-external-dtd  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://javax.xml.XMLConstants/property/accessExternalDTD  | org/mozilla/javascript/xmlimpl/XmlProcessor.java  |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet  | org/mozilla/javascript/xmlimpl/XmlProcessor.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: True 找到 1 个唯一证书 主题: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore 签名算法: rsassa\_pkcs1v15 有效期自: 2019-10-11 02:39:57+00:00 有效期至: 2841-02-23 02:39:57+00:00 发行人: C=inject, ST=inject, L=inject, O=inject, OU=inject, CN=inject.keystore 序列号: 0x47f931c3 哈希算法: sha256 md5值: 64843786c6ada15ca4254f4da77e4978 sha1值: b2e643d00042e8e23481794e88eedd3966c65dfa sha256值: 28afa96de62296ef3b7598b27d00b673920d3e0bf5fad9c95ad4ef8de5d8df99 sha512值: 2bcfcb9c6759eb8689d05d7f2393725c1ebea61bf8c4559c9057dc654ad28c1c776ddbe55a6f8a6af71968f2883555e7a74e6c588854a5a2c275ddb4cf0536d2 公钥算法: rsa 密钥长度: 1024 指纹: 61cc7d71417395a5265a787e508b72c4fdc6d6d0107c97d17221206671ae528f**

## **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.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.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.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.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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.INJECT\_EVENTS | 合法 | 按键和控制按钮 | 允许应用程序将其自己的输入事件（按键等）传递给其他应用程序。恶意应用程序可以利用它来接管电话 |
| 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.WRITE\_SECURE\_SETTINGS | 系统需要 | 修改安全系统设置 | 允许应用程序修改系统固定好设置数据。不供普通应用程序使用 |
| android.permission.BIND\_ACCESSIBILITY\_SERVICE | 合法 |  | AccessibilityService 必须要求,以确保只有系统可以绑定到它 |
| android.permission.CHANGE\_COMPONENT\_ENABLED\_STATE | 系统需要 | 启用或禁用应用程序组件 | 允许应用程序更改是否启用另一个应用程序的组件。恶意应用程序可以使用它来禁用重要的电话功能。重要的是要小心许可,因为它可能使应用程序组件进入不可用,不一致或不稳定的状态 |
| 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.REAL\_GET\_TASKS | 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.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.SET\_ACTIVITY\_WATCHER | 合法 | 监视和控制所有应用程序的启动 | 允许应用程序监视和控制系统如何启动活动。恶意应用程序可能会完全破坏系统。此权限仅用于开发,从不用于普通手机使用 |
| android.permission.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| android.permission.DELETE\_PACKAGES | 系统需要 | 删除应用程序 | 允许应用程序删除 Android 包。恶意应用程序可以使用它来删除重要的应用程序 |
| 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.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.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.BLUETOOTH\_PRIVILEGED | 系统需要 |  | 允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或消息访问。这不适用于第三方应用程序 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CLEAR\_APP\_CACHE | 系统需要 | 删除所有应用程序缓存数据 | 允许应用程序通过删除应用程序缓存目录中的文件来释放手机存储空间。访问通常非常受限于系统进程。  |
| 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.DISABLE\_KEYGUARD | 正常 |  | 如果键盘不安全,允许应用程序禁用它。 |
| android.permission.MODIFY\_PHONE\_STATE | 系统需要 | 修改电话状态 | 允许应用程序控制设备的电话功能。具有此权限的应用程序可以切换网络,打开和关闭电话收音机等,而无需通知您 |
| 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.CLEAR\_APP\_USER\_DATA | 合法 | 删除其他应用程序数据 | 允许应用程序清除用户数据 |
| android.permission.BATTERY\_STATS | 合法 | 修改电池统计信息 | 允许修改收集的电池统计信息。不供普通应用程序使用 |
| android.permission.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| android.permission.WRITE\_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |
| android.permission.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.READ\_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| android.permission.READ\_HISTORY\_BOOKMARKS | 危险 | 读取浏览器历史和书签 | 允许应用程序读取所有的URL,浏览器访问过的所有浏览器的小号书签 |
| android.permission.WRITE\_APN\_SETTINGS | 危险 | 写入访问点名称设置 | 允许应用程序修改 APN 设置,例如任何 APN 的代理和端口 |
| android.permission.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| android.permission.WRITE\_CALL\_LOG | 危险 |  | 允许应用程序写入（但不读取）用户号召日志数据。 |
| android.permission.WRITE\_VOICEMAIL | 合法 |  | 允许应用程序修改和删除系统中现有的语音邮件 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.BIND\_VPN\_SERVICE | 合法 |  | VpnService 必须要求,以确保只有系统可以绑定到它 |
| 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.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 |

## **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。**