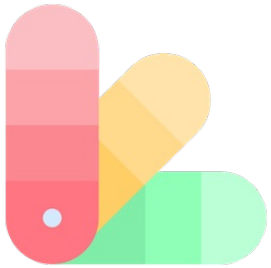
MoGua

观色配色 1.051.APK 分析报告



APP名称: 观色配色

包名:	com.joey.colors
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年9月1日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: com.joey.colors.apk
文件大小: 18.32MB
MD5值: 24cc0802b77e120b2c6b497547f4f5f3
SHA1值: abe429077a13cf38b8c2236e98296cff1fb9c217
SHA256值: 0ed01f0f299f88ac63eb6a1db0b342f708d95a6ac1108dfb205be5bdb563dee0

APP 信息

App名称: 观色配色
包名: com.joey.colors
主活动Activity: com.joey.colors.SplashActivity
安卓版本名称: 1.051
安卓版本: 51

域名线索

URL线索

邮箱线索

手机线索

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: CN=joey

签名算法: rsassa_pkcs1v15
有效期自: 2016-09-29 11:32:37+00:00
有效期至: 2041-09-23 11:32:37+00:00
发行人: CN=joey
序列号: 0x57ecfbd5
哈希算法: sha1
md5值: 01b6e72982362fb5ef501f432b4ff5f3
sha1值: 8a3eba7605f6e7b15fe669854456b6dcac2c506c
sha256值: 0b8202391a9259d2a037ff8c81d034ba0047fc5bb4ae2c82ab2838377b333cbc
sha512值: b734117c4927d8ca3e7e0033a0c8258d32f06dd2d3abbf9a6dbd5f373dff70467d430e6f281f3b74d0fc16f535be90e7199e420847a2c064ba6f4505f37b4f07
公钥算法: rsa
密钥长度: 1024
指纹: 5b1a2c161437b8f42b93e530907981fc9619efcbd130976d7f22b2ff06c75e09

硬编码敏感信息

可能的敏感信息
"private_content" : " 1. 为确实落实保护本软件用户个人信息，未经你个人明确同意，本产品坚决不会与第三方共享或对外提供你的个人信息。   2. 相关权限说明：   (1) 多媒体读写权限：在你使用本产品时候，选择图片需要读取多媒体资源的权限，若没有你的明确授权，软件没有此权限，我们将不再继续产品功能;   (2) 摄像头权限：在你需要实时取景时候，软件会询问你时候开启摄像头权限，只有经过你的允许之后，软件才能获取到该权限，否则没法使用改功能;   (3) 录音权限：在有发布你的作品时候，你可以附加发布录制的一段语音，当你点击录制的时候，需要这个权限，你可以选择拒绝我们，不使用录音这个功能;   (4) 地理位置权限：本软件内部没有用到地理位置权限，但不排除第三方依赖库，他们使用该权限是为了了解用户特征，你可以选择拒绝，并不影响你使用该软件;   (5) 手机状态权限：软件使用过程需要知道当前网络环境，来判断是否需要加载资源，如果网络环境良好，会自动下载一些必要素材资源，你如果不提供这个权限并不影响主体功能的使用，只是使用到了才去下载而已;   (6) 设备信息权限：MAC地址、IMEI、IMSI、Android ID、设备序列号等，作为用户唯一设备标识，标记用户，当软件异常时候可根据这个信息修复问题;   (7) 软件安装列表：用户软件在闪退时候，分析手机内存情况，手机上已经有安装多少软件，空间剩余多少;   (8) 运行中的进程：由于本软件依赖的第三方SDK会启动不一样的进程，为区分是软件自身进程还是第三方进程，我们需要读取当前运行的进程，获取到它的名字，和用户个人信息无关，我们不会读取和使用其他任何运行中的用户进程。   (9) 剪切板：软件内部的输入框，内容可以由外部软件复制，进而读取了剪切板内容，该内容只是给用户自我查看。当复制应用内文本时候，会把内容写到剪切板，供其他应用使用。   (10) 自启动或关联启动：为用户在桌面上设置的小部件可以根据时间变动来刷新应用界面，应用会接收时间变化的广播，若你没打开或者正式启用桌面小部件，本应用不会接收该广播，既不会有相关的自启行为，当打开本应用内部下载文件后，会关联启动第三方的应用。   3. 详情或更多SDK获取个人信息可阅读《隐私政策》和《用户协议》 了解详细信息，如你同意以上条款，可点击同意开始接受使用我们的服务。 "
"private_title" : "User agreement and Private statement"
"setting_item_private" : "隐私"
"private_title" : "用户协议和隐私策略"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

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.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.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.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.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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.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.MEDIA_PROJECTION	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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
com.joey.colors.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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.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.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.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.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
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent101565683://,
