MoGua

小苹果 1.1.5.APK 分析报告

APP名称:	小苹果

包名:	cn.grelighting.xpg
域名线索:	0条
URL线索:	0条
邮箱线索:	0条
分析日期:	2025年5月13日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: xpgtv.apk
文件大小: 41.55MB
MD5值: 67d12de588671d28507751f6206ae3cb
SHA1值: c96611718c33695405b813faff3f8f2678e4dce8
SHA256值: 1d4a0a709269c782a8ee275350773dfce37a3d626d0d032d19d960bb888cf703

APP 信息

App名称: 小苹果
包名: cn.grelighting.xpg
主活动Activity: cn.grelighting.xpg.SplashActivity
安卓版本名称: 1.1.5
安卓版本: 115

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: False
找到 1 个唯一证书
主题: C=86, ST=Zhejiang, L=Hangzhou, O=Jsy, OU=Dev, CN=LRKB

签名算法: rsassa_pkcs1v15
有效期自: 2022-03-19 18:37:53+00:00
有效期至: 2122-02-23 18:37:53+00:00
发行人: C=86, ST=Zhejiang, L=Hangzhou, O=Jsy, OU=Dev, CN=LRKB
序列号: 0x6a73dfcb
哈希算法: sha256
md5值: f0d649a742a22d465fb1984c003f31cc
sha1值: 03e9fb1085ee99a243e655a7457d4dcb843260b6
sha256值: 132d8c2d51f764f75a17352173f090daa307d08ab606daecc6fd94740be1ea29
sha512值: e3b73b00b562f889d88fd417d5a99faba0963a7d107c9e7c15b1e9cff32056bbd1ac030a5aaa5f157d7be7c2983cda71559b33cdf434c18d0d3e79c9eb22f6e6
公钥算法: rsa
密钥长度: 2048
指纹: 965dfa54fa34438c09dc658076127450d86b74add59a8e053847f96dc64159a4

硬编码敏感信息

可能的敏感信息
"ali_auth_sms_veri_title" : "请输入 %s 收到的验证码"
"ali_auth_verification_reGetCode" : "重新获取验证码"
"com_alibc_auth_actiivty_auth_ok" : "确认授权"
"com_alibc_auth_actiivty_cancel" : "取消"
"com_alibc_auth_actiivty_get" : "获取"
"com_taobao_tae_sdk_authorize_title" : "登录授权"
"ksad_ad_default_author" : "@可爱的广告君创造的原声"
"ksad_ad_default_username" : "@可爱的广告君"
"ssp_go_auth" : "去授权"

"ssp_tb_auth" : "淘宝授权"
"ssp_tb_auth_desc" : "%1$s请求淘宝授权，授权成功之后，下单购买商品可得到佣金，您是否接受授权？"
"user_name" : "点我登录"

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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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_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.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.BROADCAST_PACKAGE_ADDED	未知	Unknown permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_CHANGED	未知	Unknown permission	Unknown permission from android reference
		Unknown	

android.permission.BROADCAST_PACKAGE_INSTALL	未知	permission	Unknown permission from android reference
android.permission.BROADCAST_PACKAGE_REPLACED	未知	Unknown permission	Unknown permission from android reference
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_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_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.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.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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference
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.GET_PACKAGE_SIZE	正常	测量应用程序存储空间	允许应用程序找出任何包使用的空间
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
cn.grelighting.xpg.openadsdk.permission.TT_PANGOLIN	未知	Unknown permission	Unknown permission from android reference
		重新排序正在	

android.permission.REORDER_TASKS	正常	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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.SET_WALLPAPER	正常	设置壁纸	允许应用程序设置系统壁纸
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
miui.permission.USE_INTERNAL_GENERAL_API	未知	Unknown permission	Unknown permission from android reference
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.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.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定
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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_WIFI_MULTICAST_STATE	正常	允许Wi-Fi多播接收	允许应用程序接收不是直接发送到您设备的数据包。这在发现附近提供的服务时很有用。它比非多播模式使用更多的功率
cn.grelighting.xpg.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.alibaba.baichuan.android.trade.ui.AlibcBackActivity	Schemes: alisdk://,
com.huawei.openalliance.ad.activity.PPSLauncherActivity	Schemes: hwpps://, Hosts: cn.grelighting.xpg,

---