MoGua

顺欣茶坊 1.1.22.APK 分析报告

APP名称:	顺欣茶坊

包名:	com.djbkoeo.org
域名线索:	3条
URL线索:	2条
邮箱线索:	5条
分析日期:	2025年6月19日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 50718e013cd105bfbc6182aa2dd16472.apk
文件大小: 77.12MB
MD5值: a068557407e917cfc1a78d23d01025f5
SHA1值: 54a20bc0a6173a57ff0cd3525a9cdb96fd09da76
SHA256值: 68d5eda06ad40e9ead1a108c551b0e8659572fd9dd4b49ece141b08845d35220

APP 信息

App名称: 顺欣茶坊
包名: com.djbkoeo.org
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 1.1.22
安卓版本: 1

域名线索

域名	服务器信息
www.apple.com	**IP**: 221.194.154.187 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
crbug.com	**IP**: 216.239.32.29 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514

URL线索

URL信息	Url所在文件
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/arm64-v8a/libcocos2djs.so
https://www.openssl.org/docs/faq.html	lib/arm64-v8a/libcocos2djs.so
https://crbug.com/v8/8520	lib/arm64-v8a/libcocos2djs.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos2djs.so
https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/libcocos2djs.so
https://crbug.com/v8/8520	lib/armeabi-v7a/libcocos2djs.so

邮箱线索

邮箱地址	所在文件
cdvh@ucxrl.èr u.@p.9v	摸瓜V2引擎
1f.z@vyp.tz	摸瓜V2引擎
hb@t.lk g@bcv3.6k	摸瓜V2引擎

g@bcy5.ok	
cocos@cocoss-macbook-pro.local	lib/arm64-v8a/libcocos2djs.so
cocos@cocoss-macbook-pro.local	lib/armeabi-v7a/libcocos2djs.so

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: C=cn, ST=shanhai, L=shanhai, O=oemgle, OU=servyes, CN=zncmkin2.keystore
签名算法: rsassa_pkcs1v15
有效期自: 2023-08-27 16:34:31+00:00
有效期至: 2033-07-05 16:34:31+00:00
发行人: C=cn, ST=shanhai, L=shanhai, O=oemgle, OU=servyes, CN=zncmkin2.keystore
序列号: 0x16f2d481
哈希算法: sha256
md5值: 0973a02a2195454f4dfe8158e81a15a3
sha1值: 44a8e7475337eae3489d88c895e742b99cc1a2c5
sha256值: f7532c2ee8293390ace0acd30d4f74b85a7189ef81a950e2f0a8cff0cad10302
sha512值: 2e10275c69fcb15b377e378449b9841c9f44ff5df2f5b1d906ed02a2bca74addf52066917a71c6880f6fdacfb709ab9c8da26f4050cfa3ccc5222d4cf6f35f29
公钥算法: rsa
密钥长度: 1024
指纹: 16e891181b9698506644f5d5dae12e6bc9b64d9e7589c9d9c25abbf7221af9b5

硬编码敏感信息

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
com.aides.brother.brotheraides	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.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_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.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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作
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.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
org.cocos2dx.javascript.AppActivity	Schemes: djbkoeo://, Hosts: gameapp, Ports: 8000, Paths: /gamedetail,

---