



盛世娱乐 7.0.3.APK 分析报告



APP名称:

盛世娱乐

包名:	com.shengshi.hy
域名线索:	4条
URL线索:	1条
邮箱线索:	1条
分析日期:	2025年4月23日
分析平台:	摸瓜APK反编译平台

文件名: 3f4308f6bc1f45dd936dfd5ec0c062d.apk
文件大小: 18.17MB
MD5值: ec19fce8dd7078a1cc5e573fe16b16b7
SHA1值: 978cba9c90300b2b98b44b20bf463babf90a15c0
SHA256值: b8297237ddffea16bdf657b6506d7d6ebbe78afe6a34f655aea01f4fbd8f790b

i APP 信息

App名称: 盛世娱乐
包名: com.shengshi.hy
主活动Activity: com.haowan.lele.AppActivity
安卓版本名称: 7.0.3
安卓版本: 703

🔍 域名线索

域名	服务器信息
www.baidu.com	IP: 110.242.69.21 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
www.cocos2d-x.org	IP: 54.241.49.5 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
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
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.baidu.com/index.php/api/index/shouquan	lib/armeabi-v7a/libcocos2dlua.so
http://www.cocos2d-x.org/filedown/cocos-reader	lib/armeabi-v7a/libcocos2dlua.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libcocos2dlua.so
https://www.openssl.org/docs/faq.html	lib/armeabi-v7a/libcocos2dlua.so

 邮箱线索

邮箱地址	所在文件
cocos@cocoss-macbook-pro.local	lib/armeabi-v7a/libcocos2dlua.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=adminm7i3pq, ST=adminm7i3pq, L=adminm7i3pq, O=adminm7i3pq, OU=adminm7i3pq, CN=adminm7i3pq
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-29 11:30:51+00:00
有效期至: 2125-03-05 11:30:51+00:00
发行人: C=adminm7i3pq, ST=adminm7i3pq, L=adminm7i3pq, O=adminm7i3pq, OU=adminm7i3pq, CN=adminm7i3pq
序列号: 0x1152ff13
哈希算法: sha256
md5值: bab8614d03c61749b43cf55709826e58
sha1值: 703c5b7e6bdd81d0b518a2429a769bc0d1906c65
sha256值: 8f500878185e2a15b1ceb0914e6264f18675dd3e9cd4b463f886b5a9c1315170
sha512值: 16c7bc2f06ae7a1f5399ff468a4b2dd9bc1f22ec5db8c7cc452626408c0795c05cbe273b11fa4d9a85763ca7e8ce7876338536580af1c7e9f1d35ef56114b0f7
公钥算法: rsa
密钥长度: 1024
指纹: 1d35755835b8135c7f4506ff1d348614a36116dd18e755edf739f44d3a507b9a

硬编码敏感信息

可能的敏感信息
"com.baidu.lbsapi.API_KEY" : "123"
"openinstall_app_key" : "123"
"weixin_app_secret" : "e23181ba84a9941f2ae2033348d7b6b1"

"xianliao_app_secret": "123"

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.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.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_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
com.android.browser.permission.READ_HISTORY_BOOKMARKS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_SMS	危险	接收短信	允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示
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.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.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.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_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.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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
android.permission.SEND_SMS	危险	发送短信	允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价

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.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
org.simalliance.openmobileapi.SMARTCARD	未知	Unknown permission	Unknown permission from android reference
android.permission.NFC	正常	控制近场通信	允许应用程序与近场通信 (NFC) 标签,卡和读卡器进行通信
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.haowan.lele.AppActivity	Schemes: qp-haotianqipai://, py7kgh://,
com.tencent.tauth.AuthActivity	Schemes: 123://,
com.haowan.lele.sgapi.SGEntryActivity	Schemes: paraches://,

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。