MoGua

澳门威尼斯人 3.0.0.APK 分析报告

APP名称: 澳门威尼斯人

包名:	com.aweproject.app.amsb
域名线索:	3条
URL线索:	3条
邮箱线索:	0条
分析日期:	2025年6月12日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: amsb-app.apk
文件大小: 31.13MB
MD5值: 5e073c887745d7e894ccc47ba222d8dd
SHA1值: 830cd1a2b11c0e5014b7a3b026b1500020a8a8ef
SHA256值: 033a80ce90f77f59850da66793a5a96a78e9ee0c74ac66b74ccfaabfa0e22c94

APP 信息

App名称: 澳门威尼斯人
包名: com.aweproject.app.amsb
主活动Activity: com.aweproject.MainActivity
安卓版本名称: 3.0.0
安卓版本: 31

域名线索

域名	服务器信息
202.172.18.226	**IP**: 202.172.18.226 **所属国家**: Thailand **地区**: Krung Thep Maha Nakhon **城市**: Bangkok **纬度**: 13.749976 **经度**: 100.516815
codepush.appcenter.ms	没有服务器地理信息.
www.openl.cn	没有服务器地理信息.

URL线索

URL信息	Url所在文件
https://www.openl.cn/aas/apk.json	com/aweproject/apkupdata/ApkDownInstall.java
https://codepush.appcenter.ms/	com/microsoft/codepush/react/CodePush.java
http://no_return/	wendu/dsbridge/game/GameActivity.java
http://202.172.18.226/	wendu/dsbridge/game/GameActivity.java
https://no_return/	wendu/dsbridge/game/GameActivity.java
https://202.172.18.226/	wendu/dsbridge/game/GameActivity.java

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: CN=Tian Xia
签名算法: rsassa_pkcs1v15
有效期自: 2019-01-06 09:06:50+00:00
有效期至: 2043-12-31 09:06:50+00:00
发行人: CN=Tian Xia
序列号: 0x6e820f38
哈希算法: sha256

md5值: 295067cf475aa9ce872fe30f3d65ba40
sha1值: 8bbbeae32c7a0ca8be2a28b638072e6c6e56c2e6
sha256值: 9f3bdde1e10ae1559b73b7969057bf81343e17811dc1d6e58e0fbfa0d70a8bb5
sha512值: 31e8085a2c0eadf55cd92e826f4277a08e8d4f58c4b7ff359a22f0d2dae28c852b0270958a941767d04432fe6c6e320e25ed746fe9c42505a140c66f655093e1
公钥算法: rsa
密钥长度: 2048
指纹: 0b45f8d7ee332cc27356c432d7e01b456d5073130894485d18e4bce0ccda3692

硬编码敏感信息

可能的敏感信息
"reactNativeCodePush_androidDeploymentKey" : "deployment-key-here"

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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_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_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_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.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.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.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.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.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_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.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.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

应用内通信
