MoGua

澳门银河 8.3.2.APK 分析报告

APP名称: 澳门银河

包名:	com.LSoIBsWmMy66cnTG.BxIEcpUXQVbzzvsD
域名线索:	11条
URL线索:	3条
邮箱线索:	3条
分析日期:	2025年7月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: yinhe-p8YYS-v4e444312.apk
文件大小: 69.05MB
MD5值: 01877b286a58ca7d0502da02b68e6936
SHA1值: f99ede8085dc20a244da05123644f65a2d26cc11
SHA256值: e1b308108ed421b071c7a4a11cb51b99c3d806066e7bbd0660965898183a6c87

APP 信息

App名称: 澳门银河
包名: com.LSolBsWmMy66cnTG.BxlEcpUXQVbzzvsD
主活动Activity: org.cocos2dx.javascript.AppActivity
安卓版本名称: 8.3.2
安卓版本: 832

域名线索

域名	服务器信息
heycam.github.io	**IP**: 185.199.111.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
www.w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore

	城市: Singapore **纬度**: 1.289987 **经度**: 103.850281
dom.spec.whatwg.org	IP: 165.227.248.76 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605
purl.eligrey.com	IP: 104.236.163.66 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
cdn.jsdelivr.net	IP: 46.82.174.69 **所属国家**: Germany **地区**: Niedersachsen **城市**: Braunschweig **纬度**: 52.266121 **经度**: 10.526730
www.cocos.com	IP: 218.11.0.24 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
www.khronos.org	IP: 159.65.181.57 **所属国家**: United States of America **地区**: New Jersey **城市**: Clifton **纬度**: 40.858585 **经度**: -74.163605

www.saxproject.org	**IP**: 204.68.111.100 **所属国家**: United States of America **地区**: California **城市**: San Diego **纬度**: 32.799797 **经度**: -117.137047
raw.githubusercontent.com	**IP**: 185.199.111.133 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065647 **经度**: -79.891724
eligrey.com	**IP**: 104.236.163.66 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418

URL线索

URL**信息**	Url**所在文件**
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎
http://eligrey.com	摸瓜V2引擎
https://github.com/dsamarin	摸瓜V2引擎
https://github.com/eligrey/Blob.js/blob/master/LICENSE.md	摸瓜V2引擎
http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	摸瓜V2引擎

http://purl.eligrey.com/github/Blob.js/blob/master/Blob.js	摸瓜V2引擎
https://dom.spec.whatwg.org/	摸瓜V2引擎
https://heycam.github.io/webidl/	摸瓜V2引擎
https://github.com/taylorhakes	摸瓜V2引擎
https://github.com/taylorhakes/promise-polyfill/blob/master/LICENSE	摸瓜V2引擎
https://cdn.jsdelivr.net/npm/promise-polyfill@8/dist/polyfill.js	摸瓜V2引擎
http://www.cocos.com	摸瓜V2引擎
https://www.khronos.org/registry/OpenGL/extensions/ARB/ARB_texture_float.txt	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/helpers/DefaultHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ContentHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ErrorHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/LexicalHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/DeclHandler.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/ext/EntityResolver2.html	摸瓜V2引擎
http://www.saxproject.org/apidoc/org/xml/sax/DTDHandler.html	摸瓜V2引擎
http://www.cocos.com	摸瓜V2引擎
https://www.cocos.com/	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
ɱь@qwj3.ui찁	摸瓜V2引擎
ůyx@wl.olq	摸瓜V2引擎
n@o.mw j@u._cvtyg	摸瓜V2引擎

手机线索

签名证书

无法读取代码签名证书.

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.LSolBsWmMy66cnTG.BxlEcpUXQVbzzvsD.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
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.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.READ_MEDIA_VIDEO	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_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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.MANAGE_ACCOUNTS	危险	管理帐户列表	允许应用程序执行添加和删除帐户以及删除其密码等操作
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.BLUETOOTH_PRIVILEGED	系统需		允许应用程序在没有用户交互的情况下配对蓝牙设备,并允许或禁止电话簿访问或消息访问。这不适用于第三方应用程序

	要		
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.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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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_MEDIA_IMAGES	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.WRITE_SECURE_SETTINGS	系统需要	修改安全系统设置	允许应用程序修改系统固定好设置数据。不供普通应用程序使用

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.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_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.WRITE_MEDIA_STORAGE	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
org.cocos2dx.javascript.AppActivity	Schemes: default://,
com.tencent.tauth.AuthActivity	Schemes: tencent""://,
