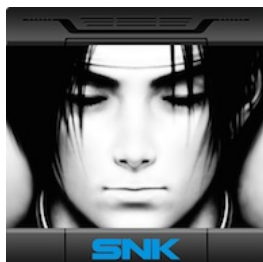




MoGua

拳皇98完整版 1.5.APK 分析报告



APP名称:

拳皇98完整版

包名:

com.snkplaymore.android007mod

域名线索:	23条
URL线索:	17条
邮箱线索:	4条
分析日期:	2025年6月14日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 102367.apk

文件大小: 71.03MB

MD5值: d80e2a807c6ef35fbf643743c056ef0b

SHA1值: 6ec5f0486ee6d4507ea5631de1ea189551cadd01

SHA256值: bc6892345553462362e3f6dd2dad6a174a62dd65e07a9d296678ec20166472a9

i APP 信息

App名称: 拳皇98完整版
包名: com.snkplaymore.android007mod
主活动Activity: com.dotemu.neogeo.kof98.KOF98InstallerActivity
安卓版本名称: 1.5
安卓版本: 26

🔍 域名线索

域名	服务器信息
ags-ext.amazon.com	IP: 44.215.137.135 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
data.flurry.com	没有服务器地理信息.
sdk.open.lbs.igexin.com	IP: 121.52.255.89 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
live.chartboost.com	IP: 13.94.30.232 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
	IP: 101.68.218.167 所属国家: China 地区: Zhejiang

sdk.open.phone.igexin.com	城市: Jiaxing 纬度: 30.752199 经度: 120.750000
developers.google.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.apple.com	IP: 60.221.218.191 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
play.google.com	IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe 纬度: 32.548328 经度: -92.045235
sdk.open.amp.igexin.com	IP: 124.160.124.197 所属国家: China 地区: Zhejiang 城市: Wenzhou 纬度: 27.999420 经度: 120.666817
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
	IP: 65.49.26.97 所属国家: United States of America 地区: Missouri

www.facebook.com	城市: Saint Louis 纬度: 38.655479 经度: -90.452339
c-hzgt2.getui.com	IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000
www.livinggames.jp	IP: 59.106.13.207 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
sdk.open.inc2.igexin.com	没有服务器地理信息.
www.chartboost.com	IP: 18.239.199.98 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
corporate.dotemu.com	IP: 51.91.73.21 所属国家: France 地区: Hauts-de-France 城市: Roubaix 纬度: 50.693710 经度: 3.174439
www.amazon.com	IP: 23.215.158.10 所属国家: Australia 地区: South Australia 城市: Adelaide 纬度: -34.928661 经度: 138.598633

pass.auone.jp	IP: 13.35.202.52 所属国家: India 地区: Telangana 城市: Hyderabad 纬度: 17.375290 经度: 78.474388
applab-sdk.amazon.com	IP: 54.239.24.8 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
d.gt.igexin.com	没有服务器地理信息.
cortana-gateway.amazon.com	IP: 52.46.132.93 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
market.android.com	IP: 142.250.217.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
s-gt.getui.com	IP: 124.160.155.55 所属国家: China 地区: Zhejiang 城市: Jiaxing 纬度: 30.752199 经度: 120.750000

URL信息	Url所在文件
https://cortana-gateway.amazon.com/cortana/gateway/getSignedDownloadUrl	com/amazon/ags/client/whispersync/migration/MigrationHttpClient.java
https://ags-ext.amazon.com/service/gamedata/WhisperData	com/amazon/ags/client/whispersync/network/WhispersyncHttpClientImpl.java
https://applab-sdk.amazon.com/1.0	com/amazon/insights/core/configuration/HttpCachingConfiguration.java
https://applab-sdk.amazon.com/1.0	com/amazon/insights/delivery/ERSRequestBuilder.java
https://applab-sdk.amazon.com/1.0	com/amazon/insights/abtest/DefaultABTestClient.java
http://corporate.dotemu.com/assets/%s/%s	com/dotemu/neogeo/kof98/KOF98InstallerActivity.java
http://developers.google.com/games/services/android/troubleshooting	com/dotemu/_3rdParty/helpers/store/GooglePlay/GameHelperUtils.java
http://pass.auone.jp/app/detail?app_id=%s	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_WorkerBee.java
http://www.livinggames.jp/sp/	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_WorkerBee.java
http://www.amazon.com/gp/mas/dl/android?p=%s&showAll=1	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_Amazon.java
https://play.google.com/store/apps/developer?id=DotEmu&referrer=utm_source%3DDotMoreGames%26utm_medium%3Dcpc%26utm_campaign%3D	com/dotemu/_3rdParty/impls/store/_3rdPartyStore_GooglePlay.java
https://www.chartboost.com/support/sdk_download/?os=ios	com/chartboost/sdk/Chartboost.java
https://live.chartboost.com	com/chartboost/sdk/impl/ba.java
http://market.android.com/	com/chartboost/sdk/impl/bb.java
http://data.flurry.com/aap.do	com/flurry/sdk/cd.java
https://data.flurry.com/aap.do	com/flurry/sdk/cd.java
http://sdk.open.phone.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://c-hzgt2.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java

http://s-gt.getui.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://d.gt.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.amp.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.lbs.igexin.com/api.htm	com/igexin/push/config/SDKUrlConfig.java
http://sdk.open.inc2.igexin.com/api.php	com/igexin/push/config/SDKUrlConfig.java
http://bi.	com/igexin/push/config/p.java
http://config.	com/igexin/push/config/p.java
http://stat.	com/igexin/push/config/p.java
http://log.	com/igexin/push/config/p.java
http://amp.	com/igexin/push/config/p.java
http://lbs.	com/igexin/push/config/p.java
http://inc.	com/igexin/push/config/p.java
http://www.facebook.com/SNK.KOFWORLD/	lib/armeabi-v7a/libEmulator.so
http://www.apple.com/DTDs/PropertyList-1.0.dtd	lib/armeabi-v7a/libEmulator.so
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libEmulator.so

 邮箱线索

邮箱地址	所在文件

support@dotemu.com	com/dotemu/installer/activities/DEInstallerActivity.java
support@dotemu.com	com/dotemu/_3rdParty/_3rdParty.java
support@dotemu.com	com/dotemu/game/base/activities/DEMainActivity.java
ftp@example.com	lib/armeabi-v7a/libEmulator.so

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=cn, ST=fujian, L=xiamen, O=4399 network co.ltd, OU=phone edit, CN=netense, E=liujiannan@4399inc.com
签名算法: rsassa_pkcs1v15
有效期自: 2014-01-06 12:19:06+00:00
有效期至: 2041-05-24 12:19:06+00:00
发行人: C=cn, ST=fujian, L=xiamen, O=4399 network co.ltd, OU=phone edit, CN=netense, E=liujiannan@4399inc.com
序列号: 0xd60be1fe821c89a9
哈希算法: sha1
md5值: 565db0bb2b9af59239651353cd9b245c
sha1值: 8cf9194e9bff321784301ee53c8ffe6aed9c9b32
sha256值: 36b1d7023ff0269ce4f321b091663e6f03d0dcd90dd7e75e577e99f2c43d56b6
sha512值: dccf3c401cadb1a3b7068a291e1dabe38a58e04e74e0bc8d62790bc4cd605c6b12949adcef9233002f4c3c9194cbbeda7c6d1597c748b3341a5d01ff65e4ebbe

硬编码敏感信息

可能的敏感信息
"openfeint_user" : "OpenFeint user"

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.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_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.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.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.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.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.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.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.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.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.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
getui.permission.GetuiService.com.snkplaymore.android007mod	未知	Unknown permission	Unknown permission from android reference
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.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
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference

应用内通信

