



MoGua

234VIP 1.1.1.APK 分析报告



APP名称:

234VIP

包名:	com.a4eec.qirs3
域名线索:	21条
URL线索:	4条
邮箱线索:	1条
分析日期:	2025年8月9日
分析平台:	摸瓜APK反编译平台

文件名: 234VIP_124.apk
文件大小: 1.49MB
MD5值: a0ea8cf2cd2165f70eaf4a8420173b49
SHA1值: b44bae804a705b7a8ad2216fbf4d1925ce5dd1f4
SHA256值: 80f3be51670b8bc509b6a6e145cf5ca77f8c6f38e86355c9d5405381f90c93e5

i APP 信息

App名称: 234VIP
包名: com.a4eec.qirs3
主活动Activity: com.example.myapplication.ui.webviewstudy.GameActivity
安卓版本名称: 1.1.1
安卓版本: 3

🔍 域名线索

域名	服务器信息
app.adjust.cn	IP: 47.104.30.117 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
schemas.android.com	没有服务器地理信息.
app.adjust.world	IP: 185.151.204.42 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037

subscription.adjust.com	IP: 185.151.204.52 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
subscription.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380
app.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
app.adjust.net.in	IP: 185.151.204.30 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
gdpr.adjust.net.in	IP: 185.151.204.30 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
subscription.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525

	经度: 13.410037
app.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
app.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380
gdpr.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
gdpr.adjust.com	IP: 185.151.204.50 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
gdpr.adjust.world	IP: 185.151.204.40 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
	IP: 185.151.204.8 所属国家: Germany

app.adjust.com	地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
gdpr.tr.adjust.com	IP: 195.244.54.5 所属国家: Turkey 地区: Izmir 城市: Izmir 纬度: 38.412731 经度: 27.138380
subscription.adjust.net.in	IP: 185.151.204.34 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
gdpr.us.adjust.com	IP: 185.151.204.70 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
subscription.adjust.world	IP: 185.151.204.44 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
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

subscription.eu.adjust.com	IP: 185.151.204.60 所属国家: Germany 地区: Berlin 城市: Berlin 纬度: 52.524525 经度: 13.410037
----------------------------	---

URL线索

URL信息	Url所在文件
https://app.adjust.com	com/adjust/sdk/Constants.java
https://gdpr.adjust.com	com/adjust/sdk/Constants.java
https://subscription.adjust.com	com/adjust/sdk/Constants.java
https://github.com/adjust/android_sdk	com/adjust/sdk/ActivityHandler.java
https://app.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://app.adjust.cn	com/adjust/sdk/network/UrlStrategy.java
https://app.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://app.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://app.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.world	com/adjust/sdk/network/UrlStrategy.java

https://gdpr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://gdpr.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.world	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.eu.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.adjust.net.in	com/adjust/sdk/network/UrlStrategy.java
https://subscription.tr.adjust.com	com/adjust/sdk/network/UrlStrategy.java
https://subscription.us.adjust.com	com/adjust/sdk/network/UrlStrategy.java
http://schemas.android.com/apk/res/android	s/AbstractC0175f.java

 邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	a0/f.java

☰ 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: O=CarracGames
签名算法: rsassa_pkcs1v15
有效期自: 2024-02-29 09:11:28+00:00
有效期至: 2074-02-16 09:11:28+00:00
发行人: O=CarracGames
序列号: 0x668297c6
哈希算法: sha1
md5值: af48adbb8dcfb090c625ee3767acb920
sha1值: 4b35427587cb20548df67097ea4417a22e675017
sha256值: ea9513d3393c3de58dbe94e734efb4e3c5db25901d2404149a290ad8e6e48f99
sha512值: 39afd92c51983310d49acaa92119bfc880b07533f3d5cfeaa45c903449418d1f1a5c4bdc70cdcb355818cd211ec287200c35b096d9c2a69ecd2b3437fc8064cb
公钥算法: rsa
密钥长度: 2048
指纹: fa1da7c34d19431238b5e1da9cf8e352737c3a30f7adb0b81b20b641e11d0feb

🔑 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
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_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.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_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.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.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.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
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.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
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.example.myapplication.ui.webviewstudy.GameActivity	Schemes: panda_124://, Hosts: open,
com.example.myapplication.ui.webviewstudy.ui.ByWebViewActivity	Schemes: https://, http://,

