



MoGua

Pro象棋 511.APK 分析报告



APP名称:

Pro象棋

包名:	vip.wqby.pro
域名线索:	2条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件名: xqpro_77982082.apk

文件大小: 72.63MB

MD5值: 051081108fb637d28c30871c9fb33c49

SHA1值: 927d9e15e7b93fd27d33b301343d82ed748d4fff

SHA256值: de5d786513870d22f2e0cf0b15367b6a47f2da09148f974486ddca208d3578c1

i APP 信息

App名称: Pro象棋

包名: vip.wqby.pro

主活动Activity: vip.wqby.pro.activity.MainActivity

安卓版本名称: 511

安卓版本: 511

🔍 域名线索

域名	服务器信息
openmp.llvm.org	IP: 54.67.122.174 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
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

🌐 URL线索

URL信息	Url所在文件
https://github.com/llvm/llvm-project/issues/.	lib/arm64-v8a/libmyapplication.so
https://github.com/opencv/opencv/issues/16739	lib/arm64-v8a/libmyapplication.so
http://openmp.llvm.org/	lib/arm64-v8a/libmyapplication.so

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: True

找到 1 个唯一证书

主题: CN=wqby, OU=wqby, O=wqby, L=wqby, ST=wqby, C=wqby

签名算法: rsassa_pkcs1v15

有效期自: 2024-12-04 10:06:02+00:00

有效期至: 2049-11-28 10:06:02+00:00

发行人: CN=wqby, OU=wqby, O=wqby, L=wqby, ST=wqby, C=wqby

序列号: 0x1

哈希算法: sha256

md5值: 2dc85e060d9a14917850b3defa876a83

sha1值: 743950786bbfd73f36883d117a912854eae2d028

sha256值: 7f6637d3eef4aae45f091043c23b9db5302238c007145bc1136f20c6f1f733f3

sha512值: 65f058a36da1da3dacd1830c0fe6501c9b7dc18cfa9f1f6486b23c71427d23d3c4f890f65b0b37313722e7f95ae565820786e488798c25253aad4e7eb2855c70

公钥算法: rsa

密钥长度: 2048

指纹: d63c7dc580bb23ba2e6200c314b2b4e198fefe95e836b356abff6ccd9b50623a

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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.SYSTEM_OVERLAY_WINDOW	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
android.permission.BIND_ACCESSIBILITY_SERVICE	合法		AccessibilityService 必须要求,以确保只有系统可以绑定到它

应用内通信

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。