MoGua

极乐园 1.0.0.APK 分析报告

APP名称:	极乐园

包名:	com.bjxpxtxu.vfpbuhadkf
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: jly.apk
文件大小: 15.44MB
MD5值: 6abe22ccf7f79be6e0b723420ca37fd6
SHA1值: c4d7843e3b27da1cb3386147add158f5a6329149
SHA256值: 13f8b847ebfffb385057a976dd4cda0d2450194cc5ccd809b00140bbc4f7ff04

APP 信息

App名称: 极乐园
包名: com.bjxpxtxu.vfpbuhadkf
主活动Activity: com.bjxpxtxu.vfpbuhadkf.SplashActivity
安卓版本名称: 1.0.0
安卓版本: 1

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
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
47.107.188.215	**IP**: 47.107.188.215 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

www.wanandroid.com	**IP**: 39.101.178.149 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583

URL线索

URL信息	Url所在文件
https://www.wanandroid.com/	com/qinyue/vcommon/http/HttpUrl.java
http://47.107.188.215:16912/api/register	com/qinyue/vmain/activity/Urls.java
http://47.107.188.215:16912/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://47.107.188.215:16912/api/subList	com/qinyue/vmain/activity/Urls.java
http://47.107.188.215:16912/api/subSmsList	com/qinyue/vmain/activity/Urls.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/MaybeLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/ObservableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/CompletableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/SingleLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/FlowableLife.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java

https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Flowable.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: True
找到 1 个唯一证书
主题: C=D1NSb, ST=mjJmw, L=V3479, O=vp1752090877478, OU=zz1752090877478, CN=aaxd
签名算法: rsassa_pkcs1v15
有效期自: 2025-07-09 19:54:37+00:00
有效期至: 2075-06-27 19:54:37+00:00
发行人: C=D1NSb, ST=mjJmw, L=V3479, O=vp1752090877478, OU=zz1752090877478, CN=aaxd
序列号: 0x49178919
哈希算法: sha512

md5值: 81a5543d918d2f0996a64bdb4c68e465
sha1值: b7abea65545e7f2c704c832b1293b89bc3416fe3
sha256值: 0dc90d12cedcd7eb869517613fea55b66207c0283a19b1af12af31fb22e5307b
sha512值: d56fdd0f4daed18f1575a9981823332f8f056930921908c65c12eac228d7fa05e5f995cc14b7696b8064d0d17abb95877cc36804efddf4fd3396dbbd5807293a
公钥算法: rsa
密钥长度: 4096
指纹: 1ba795227d7c37b6a33b001d59c79bd662fd9357ae3e2be7e28ceba6c7abbacf

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.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
android.permission.READ_SMS	危险	阅读短信或彩信	允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息
android.permission.REORDER_TASKS	正常	重新排序正在运行的应用程序	允许应用程序将任务移动到前台和后台。恶意应用程序可以在不受您控制的情况下将自己强加于前

应用内通信