MoGua

欲乐园 1.0.0.APK 分析报告

APP名称:	欲乐园

包名:	affbfedd.hecbfebe.dcddabef
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年10月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: yly.APK
文件大小: 8.34MB
MD5值: e21e93e9ba42c48cfd6abd52bd67ab33
SHA1值: da3845a17fe920c26df9549e3f6d09f8f048df5c
SHA256值: 0b33d10de6b4ed7732f9c1935bd7672e4370ba56103dfd2db4ecf8f476b43baa

APP 信息

App名称: 欲乐园
包名: affbfedd.hecbfebe.dcddabef
主活动Activity: affbfedd.hecbfebe.dcddabef.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
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
schemas.android.com	没有服务器地理信息.
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

47.106.219.233	**IP**: 47.106.219.233 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://www.wanandroid.com/	com/qinyue/vcommon/http/HttpUrl.java
http://47.106.219.233:33333/api/register	com/qinyue/vmain/activity/Urls.java
http://47.106.219.233:33333/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://47.106.219.233:33333/api/subList	com/qinyue/vmain/activity/Urls.java
http://47.106.219.233:33333/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/CompletableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/SingleLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/ObservableLife.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	com/rxjava/rxlife/FlowableLife.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/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Observable.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

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=cn, ST=cbbceieb, L=eabdbeha, O=ghabaabt, OU=fjcfijgs, CN=hbdadiir
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-08 03:42:45+00:00
有效期至: 2124-03-15 03:42:45+00:00
发行人: C=cn, ST=cbbceieb, L=eabdbeha, O=ghabaabt, OU=fjcfijgs, CN=hbdadiir
序列号: 0x2e68e026
哈希算法: sha256
md5值: 3bd812265b37fb7480ecb1b9d730640e

sha1值: b0d39e31cb1fc39991d8e7a47053cc964889e9db
sha256值: 78314f26f6db9a3df51a8ad052486bd41fb8fba1cc26b33729eeafecebb7e795
sha512值: c8e2e7c9a4ae4afa0b600655218ecc63b820fc18932ef271314e009a2abae2ef2ff6d3237a738c2f6a7afeda971ae82a1246d8895faf657e13e1c1d51567fc03
公钥算法: rsa
密钥长度: 1024
指纹: 343d9971a9337e994aa7112dedcc4e9a3a9ac82a9ba14bee75f8a51e6da9cd0c

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.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