MoGua

TCY 1.0.0.APK 分析报告

APP名称: TCY

包名:	com.xwfhfjs.fjx
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2025年6月8日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: tvip.apk
文件大小: 6.66MB
MD5值: e3243fb33bb7aed021bde1b7ba80ee18
SHA1值: 548afb210cdaa4cb9cd0af571ef2ad55f62178f0
SHA256值: 26949b7eeee346c093745085f74cd9a2d866b90af5b407288338399c0f653bf5

APP 信息

App名称: TCY
包名: com.xwfhfjs.fjx
主活动Activity: com.xwfhfjs.fjx.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**: 127.0.0.1 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
47.106.199.246	**IP**: 47.106.199.246 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
schemas.android.com	**IP**: 127.0.0.1 **所属国家**: - **地区**: -

	城市: - **纬度**: 0.000000 **经度**: 0.000000
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
https://47.106.199.246/api/register	com/qinyue/vmain/activity/Urls.java
https://47.106.199.246/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
https://47.106.199.246/api/subList	com/qinyue/vmain/activity/Urls.java
https://47.106.199.246/api/subSmsList	com/qinyue/vmain/activity/Urls.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.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
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/Maybe.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/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=Tp7pb, ST=q2c08, L=9TWYf, O=yk1749209222394, OU=oy1749209222394, CN=podo
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-06 11:27:03+00:00

有效期至: 2075-05-25 11:27:03+00:00
发行人: C=Tp7pb, ST=q2c08, L=9TWYf, O=yk1749209222394, OU=oy1749209222394, CN=podo
序列号: 0x47cd13ee
哈希算法: sha512
md5值: bd2117cf6f527a01335001418a93d3c0
sha1值: d62eb88e41aa8519c0f086a3731270801d571110
sha256值: 11bdf4649aedfa9c7a1f960e6ff05559d59dc8ffbbb9453eea1a35901e717e32
sha512值: 744c5bfbeaddfd69f9ff043318c68ef1108a416d865427dff302ee4ec811a05187343fea580bdc4f28cdde388b421b29ab9984653280a3ea53bce14a33bdcf79
公钥算法: rsa
密钥长度: 4096
指纹: 42d40d62b95b4b5da4dbcfc39bbb07139533e77dd13405cd6f6feb46d51cbc95

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