MoGua

私密空间 1.0.0.APK 分析报告

APP名称:	私密空间

包名:	cbbfgejd.cdbdcafe.cbfdafef
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2024年5月8日
分析平台:	摸瓜反编译平台

文件信息

文件名: smkj8.APK
文件大小: 6.72MB
MD5值: 4f4718667f9ff94d17f0fcb359e19fb3
SHA1值: 8948d8f78246d4c8384152205f3c8d56c7746432
SHA256值: 5f5fe1c41dd7cd8bfad2d982a22586f2e951c49e75c9d853a6f3745877d36756

APP 信息

App名称: 私密空间
包名: cbbfgejd.cdbdcafe.cbfdafef
主活动Activity: cbbfgejd.cdbdcafe.cbfdafef.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
119.23.251.182	**IP**: 119.23.251.182 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108

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
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
https://www.wanandroid.com/	com/qinyue/vcommon/http/HttpUrl.java
http://119.23.251.182:17856/api/register	com/qinyue/vmain/activity/Urls.java
http://119.23.251.182:17856/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://119.23.251.182:17856/api/subList	com/qinyue/vmain/activity/Urls.java
http://119.23.251.182:17856/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/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/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=cieeeefb, L=bdgecdda, O=feaeahjt, OU=cfacjfas, CN=agicgbfr
签名算法: rsassa_pkcs1v15
有效期自: 2024-04-26 09:44:38+00:00
有效期至: 2124-04-02 09:44:38+00:00
发行人: C=cn, ST=cieeeefb, L=bdgecdda, O=feaeahjt, OU=cfacjfas, CN=agicgbfr
序列号: 0x9fad18c
哈希算法: sha256
md5值: 7016b2ee5d790832711175b609eba089

sha1值: b0fcb9bc77aeb176cf023d361d2eb3dd5c669552
sha256值: 4c493de0edfb1bd64175b2946ccbc24d9a01fd990aa51a1852ae2c1fa660186c
sha512值: 9a2ff6e986a76e9bcf3aff0ed0d9d175df71f81205ffa7c84cfec157218740d5a69c64b31586dcf5e75e5132f3f0c7448d66a7e6dd1a649294c7f63216e0e7c6
公钥算法: rsa
密钥长度: 1024
指纹: e02b726edaa20a4e4bf0a124fdb6e4882688ca1b335ca76127ddcd58b6ebfda2

硬编码敏感信息

加壳分析

第三方SDK

名称	分类	URL链接
glide图库	开发辅助	https://reports.exodus-privacy.eu.org/trackers/469
美国Square移动支付公司	支付辅助	https://reports.exodus-privacy.eu.org/trackers/467

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