MoGua

动态网盘 1.0.0.APK 分析报告

APP名称:	动态网盘

包名:	qh5e.vf_m.x9sm
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	Sept. 13, 2024
分析平台:	摸瓜APK反编译平台

文件信息

文件名: dtwp.APK
文件大小: 7.11MB
MD5值: 4e7449e10ecf8a9892c87196761ccedf
SHA1值: 2371b8ff8ca65d97072613f66c20eeeb21c864d9
SHA256值: ae18da83fe6c1e5885c9f99c7cd4954e77e12d7c31a3f4ea23553b66b4f52c79

APP 信息

App名称: 动态网盘
包名: qh5e.vf_m.x9sm
主活动Activity: qh5e.vf_m.x9sm.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
47.115.77.167	**IP**: 47.115.77.167 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
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.
	IP: 39.101.178.149

www.wanandroid.com	**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://47.115.77.167:16591/api/register	com/qinyue/vmain/activity/Urls.java
http://47.115.77.167:16591/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://47.115.77.167:16591/api/subList	com/qinyue/vmain/activity/Urls.java
http://47.115.77.167:16591/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
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
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=xn5478, ST=xn5478, L=xn5478, O=xn5478, OU=xn5478, CN=xn5478
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-14 13:31:46+00:00
有效期至: 2124-07-21 13:31:46+00:00
发行人: C=xn5478, ST=xn5478, L=xn5478, O=xn5478, OU=xn5478, CN=xn5478
序列号: 0x5c15b397
哈希算法: sha256
md5值: 9f29fe3dbe462a9b1b0b2f55a65c815c
sha1值: d971fbb04ba621e85398b2ad403cb120c5a65cbd

sha256值: cc3efd9bc8d3274f0495ec0a825cdc59dd49c761e104774dea2df444989707ff
sha512值: fa38e6f255c98fad98d3f6339e4f25699150d3260c07445777a3a8f16b5f6a7b0fa886913d981b1657ba4c93fcea1905bb4549e9f143c81d6924ad558aa5fc2b
公钥算法: rsa
密钥长度: 1024
指纹: dfdc88f9df6cd1e1008d07a4688531152e9156774fbf0aa113db6f4e9729b309

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