MoGua

后宫选妃 1.0.0.APK 分析报告

APP名称:	后宫选妃

包名:	h4i45.eg9qt.vefdr
域名线索:	4条
URL线索:	15条
邮箱线索:	0条
分析日期:	2024年10月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: hgxf (6).APK
文件大小: 6.82MB
MD5值: 201521ca22f2877c8cd7faedc3e17a4b
SHA1值: a4c44bcf11a41a1a3f7a07e9eec520676a58861b
SHA256值: f732ede7a585c41dc6982923084765f0a4d62717c30dfdcf6acbdab62ac8f9a5

APP 信息

App名称: 后宫选妃
包名: h4i45.eg9qt.vefdr
主活动Activity: h4i45.eg9qt.vefdr.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
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
39.108.212.97	**IP**: 39.108.212.97 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545673 **经度**: 114.068108
schemas.android.com	没有服务器地理信息.
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281

URL线索

URL信息	Url所在文件
https://www.wanandroid.com/	com/qinyue/vcommon/http/HttpUrl.java
http://39.108.212.97:16909/api/register	com/qinyue/vmain/activity/Urls.java
http://39.108.212.97:16909/api/uploadImgs	com/qinyue/vmain/activity/Urls.java
http://39.108.212.97:16909/api/subList	com/qinyue/vmain/activity/Urls.java
http://39.108.212.97:16909/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=adminex7z4e, ST=adminex7z4e, L=adminex7z4e, O=adminex7z4e, OU=adminex7z4e, CN=adminex7z4e
签名算法: rsassa_pkcs1v15
有效期自: 2024-10-16 14:56:30+00:00
有效期至: 2124-09-22 14:56:30+00:00
发行人: C=adminex7z4e, ST=adminex7z4e, L=adminex7z4e, O=adminex7z4e, OU=adminex7z4e, CN=adminex7z4e
序列号: 0xf44c620
哈希算法: sha256
md5值: e519f14b1f57c72fbe279a4c95ff23a0
sha1值: 17f1a7ea1d28e383f07e0e08a251dc69b6b6be7d

sha256值: f06936ea02fb540bad67dcdebad0dd67bb1fd2be9ead131ebff2115c80215aca
sha512值: c682c1ffe5fae644802f85867c1a759f9dbdac924f4529f524e6a097b0f1fefbf07899e52cf2446d9ea473a16daaee1c07385d746202c12528c3d35285a16cb8
公钥算法: rsa
密钥长度: 1024
指纹: 540f1bc6f45bb1311d87a320d267e3e0342bc121cde048446eb28c0e17fa8ea6

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