MoGua

私信通 7.2.APK 分析报告

APP名称:	私信通

包名:	com.xingin.xhs.hk
域名线索:	2条
URL线索:	9条
邮箱线索:	0条
分析日期:	2025年7月7日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 8.46版本.apk
文件大小: 1.69MB
MD5值: 8356bcdca5653175c5360df6857e24b5
SHA1值: dfa0e796e6472a9ef82871be54997f9767410436
SHA256值: 421abfb4dcd1d2d6821e264afe181abb75c1787ffac4ea60d66e5d4f0d849862

APP 信息

App名称: 私信通
包名: com.xingin.xhs.hk
主活动Activity: com.hk.MainActivity
安卓版本名称: 7.2
安卓版本: 72

域名线索

域名	服务器信息
xml.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
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

URL线索

URL信息	Url所在文件
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/O8oO888.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/AbstractC0046oO.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/OoO08o.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/O.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/rxjava3/core/Oo.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
http://xml.apache.org/xslt	com/yhao/floatwindow/utils/O8oO888.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: False
找到 1 个唯一证书
主题: C=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15

有效期自: 2021-07-02 11:20:57+00:00
有效期至: 2046-06-26 11:20:57+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x70ef3dc
哈希算法: sha256
md5值: d434e48e4561644a983a758c2a11d552
sha1值: 62fd811afecaf9f47b6fd5fb895bdb72bf995623
sha256值: e642096bd71794a7659c40c340b7e2d981ef571e29de180a1275175014ec2955
sha512值: 34ae3ac3aa3c46cf221a55d152affd3a0d961a849d0296f147b593978a190354a042a31565d742ad42310d6cd09b2555b89defc09bb329fad9de2c7441656f7d
公钥算法: rsa
密钥长度: 2048
指纹: 01479606ad8507a07dea40440e2a78bf2aaf72a243aaa6c03e6ccf54937e7fcd

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.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.DISABLE_KEYGUARD	正常		如果键盘不安全,允许应用程序禁用它。
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

应用内通信