



MoGua

3P 8.1.7.APK 分析报告



APP名称:

3P

包名: com.hxYmpeErtTnDXPis.LmSWMtBgYrPJyjOm

域名线索: 8条

URL线索: 9条

邮箱线索: 0条

分析日期: 2025年8月4日

分析平台: [摸瓜APK反编译平台](#)

文件名: 3pzb-p8YYG-v42d5d627-x64.apk
文件大小: 51.65MB
MD5值: 0a77815b368df23a8d470e9ed055a0af
SHA1值: dfede562fcd18612d018aa9009944a44ef33bb8f
SHA256值: 01dcb9efec2953874715e1008b6d7aed7b6c22897e58322d3b9073e6d6fef3d7

i APP 信息

App名称: 3P
包名: com.hxYmpeErtTnDXPis.LmSWMtBgYrPjyjOm
主活动Activity: com.hxYmpeErtTnDXPis.LmSWMtBgYrPjyjOm.MainActivity
安卓版本名称: 8.1.7
安卓版本: 1

🔍 域名线索

域名	服务器信息
www.jsdelivr.com	IP: 104.21.23.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
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
paulbakaus.com	IP: 167.172.18.193 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
dev.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
stackoverflow.com	IP: 172.64.155.249 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.gnu.org	IP: 209.51.188.116 所属国家: United States of America 地区: Massachusetts 城市: Somerville 纬度: 42.387600 经度: -71.099503
mozilla.org	IP: 35.190.14.201 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568

URL线索

URL信息	Url所在文件
https://www.gnu.org/licenses/ >.	摸瓜V2引擎
https://www.gnu.org/licenses/ >.	摸瓜V2引擎
http://paulbikaus.com/tutorials/html5/web-audio-on-ios/	摸瓜V2引擎
http://stackoverflow.com/questions/24119684	摸瓜V2引擎
https://mozilla.org/MPL/2.0/ .	摸瓜V2引擎
https://mozilla.org/MPL/2.0/ .	摸瓜V2引擎
https://mozilla.org/MPL/2.0/ .	摸瓜V2引擎
https://www.gnu.org/licenses/ >.	摸瓜V2引擎
https://www.jsdelivr.com/using-sri-with-dynamic-files	摸瓜V2引擎
https://github.com/apvarun/toastify-js	摸瓜V2引擎
https://github.com/richttr/NoSleep.js/issues/15	摸瓜V2引擎
https://developer.mozilla.org/en-US/docs/Web/API/WakeLockSentinel/released)	摸瓜V2引擎

邮箱线索

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=CN, ST=Beijing, L=Beijing, O=cieVohwo, OU=ChuitaiN, CN=luanohQu
签名算法: rsassa_pkcs1v15
有效期自: 2025-08-03 07:26:48+00:00
有效期至: 2040-07-30 07:26:48+00:00
发行人: C=CN, ST=Beijing, L=Beijing, O=cieVohwo, OU=ChuitaiN, CN=luanohQu
序列号: 0x4300b60a5d443893
哈希算法: sha256
md5值: c554a3f1ebcb452ad64c1cabdcc4c61d
sha1值: 15cc5b787b66f75c00e17d84b749500909f7dfa5
sha256值: 5216edbd93852f056672e3c6ab65a8a8b45754948a931e6e2b33d090ae15e20c
sha512值: e8a99a44fc9d51931b3571f645ab211948416cb3eb3d0eea5d100de7357e1ba5efe8ac13023d03e7d1516d81727b05feb15a7b87afaafbae59b7cca79672cda2
公钥算法: rsa
密钥长度: 2048
指纹: 63e0ead8898e162e09073c4c14d11e4d9c6764e12349531d63abfd7eaff6a188

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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_FINE_LOCATION	危险	精细定位 (GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
	正		

android.permission.ACCESS_WIFI_STATE	常	查看Wi-Fi状态	允许应用程序查看有关 Wi-Fi 状态的信息
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.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.CAMERA	危险	拍照和录像	允许应用程序用相机拍照和录像。这允许应用程序收集相机随时看到的图像
android.permission.READ_MEDIA_AUDIO	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.READ_PHONE_STATE	危险	读取电话状态 and 身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等

android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.WAKE_LOCK	正常	防止手机睡眠	允许应用程序防止手机进入睡眠状态
android.permission.PACKAGE_USAGE_STATS	合法	更新组件使用统计	允许修改收集的组件使用统计。不供普通应用程序使用
freemme.permission.msa.SECURITY_ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由
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
com.hxYmpeErtTnDXPis.LmSWMtBgYrPjyOm.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

android.permission.REQUEST_INSTALL_PACKAGES	危险	允许应用程序请求安装包。	恶意应用程序可以利用它来尝试诱骗用户安装其他恶意软件包。
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
android.permission.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
com.asus.permission.READ_SDID_PROVIDER	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
Manifest.permission.CAPTURE_AUDIO_OUTPUT	未知	Unknown permission	Unknown permission from android reference
android.permission.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference

应用内通信