



MoGua

NJHNI 1.0.APK 分析报告



APP名称:

NJHNI

包名:	com.nsjdin.app
域名线索:	6条
URL线索:	17条
邮箱线索:	0条
分析日期:	2025年6月30日
分析平台:	摸瓜APK反编译平台

文件名: 1.apk
文件大小: 19.36MB
MD5值: f964b126703c202b754404e845b45127
SHA1值: 07c08c0363476e50b87ff3892d1d1f0909747c1a
SHA256值: 24f18f6d0911a13957e581063e837ea0048859c6ca7583530bd5d2049a90da7c

i APP 信息

App名称: NJHNI
包名: com.nsjdin.app
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
ask.dcloud.net.cn	IP: 123.125.244.81 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
schemas.android.com	没有服务器地理信息.
m3w.cn	IP: 123.6.25.115 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613

er.dcloud.net.cn	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
er.dcloud.io	没有服务器地理信息.
ns.adobe.com	没有服务器地理信息.

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	com/hjq/permissions/AndroidManifestParser.java
http://ns.adobe.com/xap/1.0/\u0000	io/dcloud/common/util/ExifInterface.java
https://m3w.cn/s/	io/dcloud/common/util/ShortCutUtil.java
https://ask.dcloud.net.cn/article/282	io/dcloud/common/constant/DOMException.java
https://ask.dcloud.net.cn/article/35058	io/dcloud/feature/audio/AudioRecorderMgr.java
https://ask.dcloud.net.cn/article/283	io/dcloud/feature/utsplugin/ProxyModule.java
https://er.dcloud.io/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://er.dcloud.net.cn/sc	io/dcloud/feature/gg/dcloud/ADHandler.java
https://ask.dcloud.net.cn/article/35627	io/dcloud/p/r.java

https://ask.dcloud.net.cn/article/35877	io/dcloud/p/r.java
https://ask.dcloud.net.cn/article/283	io/dcloud/p/h1.java
https://er.dcloud.io/rv	io/dcloud/p/d0.java
https://er.dcloud.net.cn/rv	io/dcloud/p/d0.java
https://ask.dcloud.net.cn/article/287	io/dcloud/share/IFShareApi.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifViewUtils.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextureView.java
http://schemas.android.com/apk/res/android	pl/droidsonroids/gif/GifTextView.java

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: True
找到 1 个唯一证书
主题: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2025-06-24 07:10:32+00:00
有效期至: 2055-06-24 07:10:32+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

序列号: 0x532f9d93527ef90551e764c6c54332a90d344b50
哈希算法: sha256
md5值: eae23eadcd859e7104c0fb3b0eaa52f8
sha1值: 4937da7a436853271cba2bb27909e13b402e3a66
sha256值: de6d876b66e592a7945184cabb47ecb13b626a716a48ff3bf16c42933c2b0168
sha512值: a055cc9ada492c83ae6f3ed320f526456703dde84a763aa1eda66bf9bdf81e231b027db32e2bacf1cdfaf73629a1efa95ea3d501afbf4c295013e14ce9264c4
公钥算法: rsa
密钥长度: 4096
指纹: 732e117615fbf729faaaa88f015d74dbe199a7c969ddb49cd89784729b4ad048

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

	是		
--	---	--	--

向手机申请的权限	否 危 险	类型	详细情况
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_PHONE_STATE	危险	读取电话状态和身份	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.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.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
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.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.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	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
com.nsjdin.app.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_WIFI_STATE	正常	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.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.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.VIBRATE	正常	可控震源	允许应用程序控制振动器
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.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。
com.android.vending.CHECK_LICENSE	未知	Unknown permission	Unknown permission from android reference

应用内通信