Evaluation Warning: The document was created with Spire.Doc for Python.

**小红书（ 7.53.0版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | 小红书 |
| 版本 | 7.53.0 |
| 包名 | com.xingin.xhs |
| 域名线索 | 11条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2024年9月10日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | 2\_af0c61849f6cf19ff7fd52af192ef598.apk |
| 文件大小 | 109.8MB |
| MD5值 | 6e30041897c16e17864c12c9d9e5904b |
| SHA1值 | 7f75715857a4024fe2341529b25b58476a56f53c |
| SHA256值 | e3fa23c7a7a6ae8b0bba00090c158b92b3d65fc7011702eca624f28c8f33fdab |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小红书 |
| 包名 | com.xingin.xhs |
| 主活动Activity | com.xingin.xhs.index.v2.IndexActivityV2 |
| 安卓版本名称 | 7.53.0 |
| 安卓版本 | 7530239 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| play.google.com | IP: 142.251.43.14  所属国家: United States of America  地区: California  城市: Mountain View |
| upload.ffmpeg.org | IP: 213.36.253.119  所属国家: France  地区: Ile-de-France  城市: Paris |
| store-at-dre.hispace.dbankcloud.com | IP: 80.158.5.6  所属国家: Germany  地区: Schleswig-Holstein  城市: Kiel |
| e.189.cn | IP: 42.123.76.65  所属国家: China  地区: Beijing  城市: Beijing |
| wap.cmpassport.com | IP: 120.197.235.27  所属国家: China  地区: Guangdong  城市: Guangzhou |
| sns-video-hw.xhscdn.com | IP: 123.151.96.28  所属国家: China  地区: Tianjin  城市: Tianjin |
| www.sharesdk.cn | IP: 115.227.41.64  所属国家: China  地区: Zhejiang  城市: Taizhou |
| store.hispace.hicloud.com | IP: 49.4.44.164  所属国家: China  地区: Beijing  城市: Beijing |
| www.xiaohongshu.com | IP: 212.64.115.101  所属国家: China  地区: Beijing  城市: Beijing |
| opencloud.wostore.cn | IP: 116.128.209.136  所属国家: China  地区: Shanghai  城市: Shanghai |
| appgallery.cloud.huawei.com | IP: 117.78.15.51  所属国家: China  地区: Guangdong  城市: Guangzhou |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://www.xiaohongshu.com/crown/community/advanced\_agreement?fullscreen=true | Android String Resource |
| http://sns-video-hw.xhscdn.com/351ad9a64564b75ec82eb668fd7344832208c188.mp4?v=2 | Android String Resource |
| https://play.google.com/store | Android String Resource |
| https://appgallery.cloud.huawei.com/app/ | Android String Resource |
| https://play.google.com/store/apps/details?id= | Android String Resource |
| https://appgallery.cloud.huawei.com | Android String Resource |
| https://wap.cmpassport.com/resources/html/contract.html | Android String Resource |
| https://e.189.cn/sdk/agreement/detail.do?hidetop=true | Android String Resource |
| https://opencloud.wostore.cn/authz/resource/html/disclaimer.html?fromsdk=true | Android String Resource |
| http://www.xiaohongshu.com/crown/community/terms | Android String Resource |
| http://www.xiaohongshu.com/crown/community/privacy | Android String Resource |
| https://www.xiaohongshu.com/privacy/teenager | Android String Resource |
| www.xiaohongshu.com/content\_dispute | Android String Resource |
| http://www.xiaohongshu.com/mobile/terms | Android String Resource |
| http://www.xiaohongshu.com/mobile/privacy | Android String Resource |
| http://www.sharesdk.cn | Android String Resource |
| https://store-at-dre.hispace.dbankcloud.com/hwmarket/api/ | Android String Resource |
| https://store.hispace.hicloud.com/hwmarket/api/ | Android String Resource |
| ftp://upload.ffmpeg.org/incoming/ | lib/armeabi-v7a/libswdecoder.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| qinquan@xiaohongshu.com | Android String Resource |
| ffmpeg-devel@ffmpeg.org | lib/armeabi-v7a/libswdecoder.so |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: True Found 1 unique certificates Subject: C=86, ST=shanghai, L=shanghai, O=xingin, OU=xingin, CN=xiaohongshu Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2014-07-16 08:32:34+00:00 Valid To: 2039-07-10 08:32:34+00:00 Issuer: C=86, ST=shanghai, L=shanghai, O=xingin, OU=xingin, CN=xiaohongshu Serial Number: 0x53c638a2 Hash Algorithm: sha1 md5: 6cfca61d9d1eca56844806706ba18cf7 sha1: 4ae949b443ed2e33b71f024af9ef24ff14f2e4d0 sha256: f375f0f6af7c94c364b35cd6f6a66d64aefae66e32f935b48773c0faad04c121 sha512: eeadeb0436099c9fa25e9c21b546a7a94d3261f91ecddf75a0b3f8b8688d51fd13bdcb918cf72f1d2900ed3ce73884471bce5668307532f52359e5ea4a729633 PublicKey Algorithm: rsa Bit Size: 1024 Fingerprint: ec7382d5768d97b472ac44689b5abcaf4f5a122e0144f3a1b70ec1066d30a09b**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "api" : "价格优惠" |
| "aws" : "微博" |

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| 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.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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.BROADCAST\_STICKY | 正常 | 发送粘性广播 | 允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定 |
| 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.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。 |
| com.android.launcher.permission.INSTALL\_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ\_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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\_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.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.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 |
| 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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| com.xingin.xhs.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.push.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.xingin.xhs.push.permission.MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.c2dm.permission.RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| com.xingin.xhs.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.coloros.mcs.permission.RECIEVE\_MCS\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.xingin.xhs.permission.JPUSH\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.huawei.android.launcher.permission.READ\_SETTINGS | 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.huawei.android.launcher.permission.WRITE\_SETTINGS | 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 |
| android.permission.EXPAND\_STATUS\_BAR | 正常 | 展开/折叠状态栏 | 允许应用程序展开或折叠状态栏 |
| getui.permission.GetuiService.com.xingin.xhs | 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| android.permission.WRITE\_CALENDAR | 危险 | 添加或修改日历事件并向客人发送电子邮件 | 允许应用程序添加或更改日历上的事件,这可能会向客人发送电子邮件。恶意应用程序可以使用它来删除或修改您的日历活动或向客人发送电子邮件 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| 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.READ\_CALENDAR | 危险 | 读取日历事件 | 允许应用程序读取您手机上存储的所有日历事件。恶意应用程序可以借此将您的日历事件发送给其他人 |
| com.huawei.meetime.CAAS\_SHARE\_SERVICE | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| android.permission.SET\_WALLPAPER | 正常 | 设置壁纸 | 允许应用程序设置系统壁纸 |
| 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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |
| freemme.permission.msa | 未知 | Unknown permission | Unknown permission from android reference |
| com.xingin.xhs.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.xingin.xhs.permission.PUSH\_PROVIDER | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.vending.BILLING | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.permission.PUSH | 未知 | Unknown permission | Unknown permission from android reference |
| 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 |
| com.android.vending.CHECK\_LICENSE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.xingin.xhs.routers.RouterPageActivity | **Schemes**: xhsdiscover://, http://, https://, qnpr8hbhw393f9://,  **Hosts:** login\_page, welcome\_page, store, messages, interaction\_notification, profile, webview, extweb, rn, swan, miniapp, wechat\_miniprogram, home, discovery, 1, item, multi\_note, video\_feed, note\_mix, guang, topic, homefeed, comments, portrait\_feed, post, post\_video\_album, post\_video, post\_note, notes\_draft\_box, post\_new\_note, recommend, me, user, message, red\_house, face\_photo, ar\_skin\_detection, search, page, instore\_search, poi, spv, spu, spv\_skeleton, spl, spv\_draft, \*.xiaohongshu.com, choose\_share\_user, splashshow, advert, pm, list, scenario, account, pois, general\_setting, dark\_mode\_setting, notification\_setting, report, system\_settings, callback, resource\_cache\_manage, board, live\_audience, hey, hey\_post, hey\_edit, hey\_home\_feed,  **Mime Types:** image/\*, video/\*,  **Paths:** /follow, /explore, /localfeed, /note, /store, /user, /contacts, /weibo, /profile, /my, /center, /collections, /comments, /followers, /notifications, /room, /room\_list, /room\_feed, /room\_inner\_feed, /schedule\_room, /recommend, /result, /goods\_category, /native\_template\_landingpage, /chat, /strangers, /groupchat, /login, /bind, /bind/phone,  **Path Patterns:** /.\*, /item/.\*, /category, /user/.\*, /.\*/collects, /me/collects, /.\*/followers, /me/followers, .\*, /goods/.\*, /list/.\*, /report/.\*, /board/.\*, |
| com.xingin.xhs.push.VIVOPushEmptyActivity | **Schemes**: xhsdiscover://,  **Hosts:** push,  **Paths:** /vivopush, |
| com.xingin.hey.heyshoot.HeyEditActivity | **Schemes**: @string/c93://,  **Hosts:** @string/c72, |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent100507190://, |
| com.alibaba.baichuan.android.trade.ui.AlibcBackActivity | **Schemes**: alisdk://, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**