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

**口袋48（ 6.3.2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 | 口袋48 |
| 版本 | 6.3.2 |
| 包名 | com.pocket.snh48.activity |
| 域名线索 | 23条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | pocket48.apk |
| 文件大小 | 66.77MB |
| MD5值 | fd90d389da48691bd24745c67ef750d9 |
| SHA1值 | 158078ffd3e3031dfb814e9457d63dd217505721 |
| SHA256值 | dd1c7ac1cfc0ff775583f2798a7db676e11639f2d5e245dddf945ae680fb0bc7 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 口袋48 |
| 包名 | com.pocket.snh48.activity |
| 主活动Activity | com.pocket.snh48.activity.view.splash.SplashActivity |
| 安卓版本名称 | 6.3.2 |
| 安卓版本 | 22051201 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| lbs.netease.im | IP: 59.111.239.36 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| 169.254.169.254 | IP: 169.254.169.254 所属国家: - 地区: - 城市: -  |
| 45.127.128.25 | IP: 45.127.128.25 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| yunxin.163.com | IP: 59.111.243.80 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| quality-detect.zegocloud.com | IP: 47.242.252.76 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| s3.amazonaws.com | IP: 52.216.207.21 所属国家: United States of America 地区: Virginia 城市: Ashburn  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| www.w3.org | IP: 128.30.52.100 所属国家: United States of America 地区: Massachusetts 城市: Cambridge  |
| 45.127.128.24 | IP: 45.127.128.24 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| appgallery.cloud.huawei.com | IP: 49.4.35.33 所属国家: China 地区: Beijing 城市: Beijing  |
| ..png | 没有服务器地理信息.  |
| edusuite-song.zego.im | IP: 114.132.191.128 所属国家: China 地区: Beijing 城市: Beijing  |
| 169.254.170.2 | IP: 169.254.170.2 所属国家: - 地区: - 城市: -  |
| www.apple.com | IP: 221.194.155.186 所属国家: China 地区: Hebei 城市: Langfang  |
| statistic.live.126.net | IP: 183.136.182.46 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| www.zetetic.net | IP: 13.224.141.33 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| lame.sf.net | IP: 204.68.111.100 所属国家: United States of America 地区: California 城市: San Diego  |
| ..wav | 没有服务器地理信息.  |
| doc-zh.zego.im | IP: 47.103.157.124 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.openssl.org | IP: 23.2.129.55 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| play.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| lbs.chatnos.com | IP: 59.111.239.40 所属国家: China 地区: Guangdong 城市: Guangzhou  |
| nos.netease.com | IP: 45.127.129.36 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://play.google.com/store/apps/details?id=  | Android String Resource  |
| https://appgallery.cloud.huawei.com  | Android String Resource  |
| https://www.zetetic.net/sqlcipher/  | Android String Resource  |
| https://www.zetetic.net/sqlcipher/license/  | Android String Resource  |
| https://github.com/sqlcipher/android-database-sqlcipher  | Android String Resource  |
| https://www.openssl.org/docs/faq.html  | lib/arm64-v8a/libqcOpenSSL.so  |
| http://quality-detect.zegocloud.com  | lib/arm64-v8a/libZegoExpressEngine.so  |
| https://edusuite-song.zego.im  | lib/arm64-v8a/libZegoExpressEngine.so  |
| https://doc-zh.zego.im/article/1153  | lib/arm64-v8a/libZegoExpressEngine.so  |
| https://doc-zh.zego.im/article/5670  | lib/arm64-v8a/libZegoExpressEngine.so  |
| https://doc-zh.zego.im/article/13610#1.  | lib/arm64-v8a/libZegoExpressEngine.so  |
| https://doc-zh.zego.im/article/13610#1  | lib/arm64-v8a/libZegoExpressEngine.so  |
| http://s  | lib/arm64-v8a/libZegoExpressEngine.so  |
| ftp://%s:%s@%s  | lib/arm64-v8a/libZegoExpressEngine.so  |
| http://lame.sf.net  | lib/arm64-v8a/libZegoExpressEngine.so  |
| http://www.w3.org/XML/1998/namespace  | lib/arm64-v8a/liblibpag.so  |
| http://www.w3.org/2000/xmlns/  | lib/arm64-v8a/liblibpag.so  |
| https://statistic.live.126.net  | lib/arm64-v8a/libhigh-available.so  |
| https://lbs.netease.im/lbs/conf.jsp  | lib/arm64-v8a/libhigh-available.so  |
| https://lbs.chatnos.com/lbs/conf.jsp  | lib/arm64-v8a/libhigh-available.so  |
| https://yunxin.163.com/lbs/conf.jsp  | lib/arm64-v8a/libhigh-available.so  |
| http://45.127.128.24  | lib/arm64-v8a/libhigh-available.so  |
| http://45.127.128.25  | lib/arm64-v8a/libhigh-available.so  |
| http://nos.netease.com  | lib/arm64-v8a/libhigh-available.so  |
| http://s3.amazonaws.com/doc/2006-03-01/  | lib/arm64-v8a/libhigh-available.so  |
| http://www.w3.org/2001/XMLSchema-instance  | lib/arm64-v8a/libhigh-available.so  |
| http://169.254.170.2  | lib/arm64-v8a/libhigh-available.so  |
| http://169.254.169.254  | lib/arm64-v8a/libhigh-available.so  |
| http://www.apple.com/DTDs/PropertyList-1.0.dtd  | lib/arm64-v8a/libZegoEffects.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| ftp@example.com appro@openssl.org  | lib/arm64-v8a/libZegoExpressEngine.so  |
| ftp@example.com  | lib/arm64-v8a/libhigh-available.so  |

### **4.4 手机号线索**

## **5. 签名证书**

**APK is signed v1 signature: True v2 signature: True v3 signature: False Found 1 unique certificates Subject: C=86, ST=Shanghai, L=Shanghai, O=Nine Style, OU=Nine Style, CN=FangWen Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2014-12-19 04:15:49+00:00 Valid To: 2064-12-06 04:15:49+00:00 Issuer: C=86, ST=Shanghai, L=Shanghai, O=Nine Style, OU=Nine Style, CN=FangWen Serial Number: 0x47f42172 Hash Algorithm: sha256 md5: 1b832cea056f506e6dc228201fe02080 sha1: f44b9f1a173564cd686d7fbf6022235ebfe49c48 sha256: a4154e5987fe5fe2eab5f59c451dfbbf3f5929d49f13c18805ad32dafb994335 sha512: 05e2f284cd3efa047cf2880b5789413f6acccce318d12aec30ceab58d384a67fa03c8a50ef7e9eb83ef4e0daff9865cb96b545dbdb8f0f674c4c1c0bab53b66c PublicKey Algorithm: rsa Bit Size: 2048 Fingerprint: 994d2c13258234ec7e8f4c3e15f12e4da95ec210ba766345b98b2f9ee23ac63c**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "cmbkb\_publickey" : "aP28KufJh9SXSNjAa/8uUmY0xWKImkTaQVcQACeXGK44QOLAbYo4F+2TQ2O010DHwMAPAq8OeELxHK6BTAaxVUao4jOiCFSqpnoZ0MH4U58kgq9RoAkcSskUAVEtJT16w8UoguX6VTYjJ/EWOwaRNcxb4taIPi6S8AnwTXfniIeuzo1LsMOLlACY3+PAQJDYO4/47Wf/cTDB9Fqu6J7ab9+EueLsBrWR0uQ/h+ANM+VE19s7UikisumSd06fIg8aOFORj/1zjmWMi8u+7FESFYywROQVcd+v8HCJoKnVdJQaAd3Nu4cVx+34PE3K46UqyTi36JkvGX6ZZDK/ImRukQ=="  |
| "fix\_password" : "修改密码"  |
| "library\_android\_database\_sqlcipher\_author" : "Zetetic, LLC"  |
| "library\_android\_database\_sqlcipher\_authorWebsite" : "https://www.zetetic.net/sqlcipher/"  |
| "past\_session" : "以往场次"  |
| "private\_letter" : "私信"  |
| "private\_protocol" : "您在使用我们的服务时，我们可能会收集和使用您的相关信息。我们希望通向您说明 1、在使用我们的服务时，我们如何收集、使用、储存和分享这些信息 2、我们为您提供的访问、更新、控制和保护这些信息的方式。我们非常重视您的个人信息保护，关于详细的信息可以访问《隐私政策》进一步了解。"  |
| "private\_tip" : "我们仅会将您的信息用于提供服务和改善体验，我们将区里保障您的信息安全，请同意后使用。"  |
| "revise\_password" : "修改密码"  |
| "shop\_pay\_way\_sigua\_forget\_password" : "忘记密码？"  |
| "wbcf\_user\_auth\_protocol\_name" : "《个人信息处理授权书》"  |

## **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.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 |
| 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。 |
| com.pocket.snh48.activity.permission.RECEIVE\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.pocket.snh48.activity.permission.PROCESS\_PUSH\_MSG | 未知 | Unknown permission | Unknown permission from android reference |
| com.pocket.snh48.activity.permission.MIPUSH\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| 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.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.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.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| com.pocket.snh48.activity.andpermission.bridge | 未知 | Unknown permission | Unknown permission from android reference |
| com.pocket.snh48.activity.permission.PUSH\_PROVIDER | 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 |
| com.huawei.appmarket.service.commondata.permission.GET\_COMMON\_DATA | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.pocket.snh48.mine.ui.certify.alipay.AlipayCertfyActivity | **Schemes**: snh48://, **Hosts:** login, **Paths:** /zimaauth,  |
| com.tencent.tauth.AuthActivity | **Schemes**: tencent1103838320://,  |
| com.pocket.snh48.base.ui.proxy.UriProxyActivity | **Schemes**: snh48://,  |

**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。**