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

**小迪渗透吧（ 1.0.0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 | 小迪渗透吧 |
| 版本 | 1.0.0 |
| 包名 | com.xiaodi8.app.xaverrw |
| 域名线索 | 11条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年5月13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 | xiaodi8.apk |
| 文件大小 | 3.23MB |
| MD5值 | 84ef9c687e80c924ab856e93035577fe |
| SHA1值 | 1ccb345166310651b33bb3f0f5b06b438c9b754e |
| SHA256值 | c84ae05c2614b236f255352739553dc329f0760e9d4112ca56b2d32312a4dad4 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 小迪渗透吧 |
| 包名 | com.xiaodi8.app.xaverrw |
| 主活动Activity | com.lt.app.MainActivity |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 100 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.gstatic.com | IP: 203.208.50.34  所属国家: China  地区: Beijing  城市: Beijing |
| www.xiaodi8.com | IP: 47.75.212.155  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| i.yimenyun.net.09aea97b.cdnhwc8.cn | IP: 125.39.165.87  所属国家: China  地区: Tianjin  城市: Tianjin |
| schemas.android.com | 没有服务器地理信息. |
| android.googlesource.com | IP: 74.125.204.82  所属国家: United States of America  地区: California  城市: Mountain View |
| hcdnw101.sme.cdnhwcaip122.cn | IP: 125.39.165.87  所属国家: China  地区: Tianjin  城市: Tianjin |
| g.yimenseo.net | IP: 39.100.95.75  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| gn.emen.ltd | IP: 39.100.76.72  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| xiaodi8.com | IP: 47.75.212.155  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| i.yimenyun.net | IP: 125.39.165.87  所属国家: China  地区: Tianjin  城市: Tianjin |
| edgedl.me.gvt1.com | IP: 34.104.35.123  所属国家: United States of America  地区: California  城市: Mountain View |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android | e/g/d/f/k.java |
| www.gstatic.com | 摸瓜V3引擎 |
| i.yimenyun.net.09aea97b.cdnhwc8.cn | 摸瓜V3引擎 |
| instantmessaging-pa.googleapis.com | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| i.yimenyun.net | 摸瓜V3引擎 |
| content-autofill.googleapis.com | 摸瓜V3引擎 |
| hcdnw101.sme.cdnhwcaip122.cn | 摸瓜V3引擎 |
| gn.emen.ltd | 摸瓜V3引擎 |
| xiaodi8.com | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| www.xiaodi8.com | 摸瓜V3引擎 |
| clientservices.googleapis.com | 摸瓜V3引擎 |
| g.yimenseo.net | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| infinitedata-pa.googleapis.com | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm | 摸瓜V3引擎 |
| play.googleapis.com | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/clang | 摸瓜V3引擎 |
| update.googleapis.com | 摸瓜V3引擎 |
| edgedl.me.gvt1.com | 摸瓜V3引擎 |

### **4.3 邮箱线索**

### **4.4 手机号线索**

## **5. 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=WX, ST=WX, L=WX, O=WX, OU=WXBB, CN=WX 签名算法: rsassa\_pkcs1v15 有效期自: 2023-03-28 07:46:10+00:00 有效期至: 2123-03-04 07:46:10+00:00 发行人: C=WX, ST=WX, L=WX, O=WX, OU=WXBB, CN=WX 序列号: 0x43218386 哈希算法: sha256 md5值: f42dbfa50b6e7f36a5f267afb7ecf157 sha1值: 89770da163dbb403da7de3c80b4819e36d8246ad sha256值: 2251b24a710c622704d5b9f74e241c1cd3b24e75182eef9f1b492c4ae7c6e9b5 sha512值: bcb491983a4c6a5f080997a94cea1613ec88a6c3a7728681587b929c1d687b8546806ab37bb6890d5991fe1f283be7bd4369a752de30fda528021e6b220a1358 公钥算法: rsa 密钥长度: 2048 指纹: 2e34a7824ab13815441d97b0c3142768e02b74cbcb8550687f0fa3062b21a16d**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "p\_rcpush\_mzAppKey" : "" |
| "p\_rcpush\_opAppKey" : "" |
| "p\_rcpush\_opAppSecret" : "" |
| "p\_rcpush\_vvAppKey" : "" |
| "p\_rcpush\_xmAppKey" : "" |
| "p\_weibo\_appkey" : "" |

## **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.RECEIVE\_USER\_PRESENT | 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.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.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.SYSTEM\_OVERLAY\_WINDOW | 未知 | Unknown permission | Unknown permission from android reference |
| com.xiaodi8.app.xaverrw.permission.YM\_APP | 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.RECORD\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| 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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.lt.app.JumpActivity | **Schemes**: ltapp335195://, |

**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。**