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

**⁡⁡F⁡o⁡x⁡⁡⁡（ null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 | ⁡⁡F⁡o⁡x⁡⁡⁡ |
| 版本 | null |
| 包名 | odb.gbznzvd1.nat |
| 域名线索 | 2条 |
| URL线索 | 2条 |
| APP图标 |  |
| 分析日期 | 2025年6月16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 | Fox-JiMB4uxNWDqpQAC2.apk |
| 文件大小 | 21.53MB |
| MD5值 | 8c43e686c743aa0e61cf3a1f70ffe00f |
| SHA1值 | 1b9e06b49e44bcf00d405abd9d8b3465185bc640 |
| SHA256值 | 8500bdeafa0f66d036f4d1e52fc31ff866b57a769e319971d69c4cce8d66de27 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | ⁡⁡F⁡o⁡x⁡⁡⁡ |
| 包名 | odb.gbznzvd1.nat |
| 主活动Activity | com.dgdg2024.app.dfdg\_app.MainActivity |
| 安卓版本名称 | null |
| 安卓版本 |  |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| developer.android.com | IP: 142.250.107.113 所属国家: United States of America 地区: California 城市: Mountain View  |
| plus.google.com | IP: 198.44.185.131 所属国家: United States of America 地区: California 城市: Los Angeles  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://developer.android.com/guide/topics/permissions/overview  | io/flutter/plugin/platform/h.java  |
| https://plus.google.com/  | s1/j1.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | p1/v.java  |

### **4.4 手机号线索**

## **5. 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=ajazvomonpyrodi, ST=rndupjcjkcxkwzp, L=ipwalgfydfgkajj, O=ube1749773231803, OU=ugf1749773231803, CN=Xvjf1749773231803 签名算法: rsassa\_pkcs1v15 有效期自: 2025-06-13 00:07:11+00:00 有效期至: 2075-06-01 00:07:11+00:00 发行人: C=ajazvomonpyrodi, ST=rndupjcjkcxkwzp, L=ipwalgfydfgkajj, O=ube1749773231803, OU=ugf1749773231803, CN=Xvjf1749773231803 序列号: 0x539c4a3a 哈希算法: sha1 md5值: 727fde930fa323048f476d716c56233e sha1值: cba98eaee7863eb54246eb52bdfd6270358dd4dd sha256值: 84c64027d70a665172e977fc08b47aaeb0ae1a786a041863ffeb934d6d165b76 sha512值: 10f42b77223ec52f3dd90a4a8704cbcd4b704acba6527b07b3937d2be291ea2e32a15fa9c25ffc026f916dffe15262beb80db6b827d921691a6eda6f6702341a 公钥算法: rsa 密钥长度: 1024 指纹: 1da8b47510ba07887b7be8c3e61f54fff2712faf63a37fbce421e095dc9f4e27**

## **6. 硬编码敏感信息**

## **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.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.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.READ\_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| 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.READ\_PHONE\_NUMBERS | 危险 |  | 允许到设备的读访问的电话号码。这是 READ\_PHONE\_STATE 授予的功能的一个子集,但对即时应用程序公开 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| android.permission.QUERY\_ALL\_PACKAGES | 正常 |  | 允许查询设备上的任何普通应用程序,无论清单声明如何 |
| 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.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.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 |
| odb.gbznzvd1.nat.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**