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

**福多多福袋助手（ 1.738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 | 福多多福袋助手 |
| 版本 | 1.738 |
| 包名 | com.android.greaderex |
| 域名线索 | 5条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年7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 | 福多多福袋助手\_1.738.apk |
| 文件大小 | 2.26MB |
| MD5值 | 31d839c24f108f71aee13544b5a329cb |
| SHA1值 | d1db3834fce9062db7eddf61e233ffd5205c4e15 |
| SHA256值 | fe2b7e4480194e987693b761891fda89691994eb873dc411128936831ae90386 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 福多多福袋助手 |
| 包名 | com.android.greaderex |
| 主活动Activity | com.android.greaderex.MainActivity |
| 安卓版本名称 | 1.738 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ask.xreader22.top | IP: 112.196.222.16 所属国家: Korea (Republic of) 地区: Gyeonggi-do 城市: Suwon  |
| update.xreader22.top | IP: 47.100.32.93 所属国家: China 地区: Shanghai 城市: Shanghai  |
| v.douyin.com | IP: 119.167.184.232 所属国家: China 地区: Shandong 城市: Qingdao  |
| schemas.android.com | 没有服务器地理信息.  |
| v.kuaishou.com | IP: 103.102.202.144 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | y/AbstractC0430b.java  |
| https://v.douyin.com/ijepW1fn/  | 摸瓜V1引擎  |
| https://v.kuaishou.com/BzU5g7/  | 摸瓜V1引擎  |
| https://v.douyin.com/ijepW1fn/:https://v.kuaishou.com/BzU5g7/  | 摸瓜V3引擎  |
| ask.xreader22.top  | 摸瓜V3引擎  |
| update.xreader22.top  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res/android  | 摸瓜V3引擎  |
| http://schemas.android.com/apk/res-auto  | 摸瓜V3引擎  |
| http://schemas.android.com/aapt  | 摸瓜V3引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| hzxsgfzl@gmail.com  | 摸瓜V1引擎  |

### **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: CN=Paddle, OU=paddlecop 签名算法: rsassa\_pkcs1v15 有效期自: 2024-05-10 00:21:37+00:00 有效期至: 2049-05-04 00:21:37+00:00 发行人: CN=Paddle, OU=paddlecop 序列号: 0x1 哈希算法: sha256 md5值: a382630005b7e2b6b1d61a3cf6a1b10a sha1值: ae0f8cf6f142e666fe62b3892033fb4f2708b423 sha256值: b0d800d984a83549dd6502c4448e93bc2f223d9f834ad8b4ba3ce991a8a328a1 sha512值: eaf5ac6d5572b6ae1618aeb45797411c9922ef1bb696709f93c0327fbfd6a59fdeef1c7ee589b097bfce3488efa4e4861e2bbe81dc79252081fd0ccc9ac42a7a 公钥算法: rsa 密钥长度: 2048 指纹: ba1d98b5b23917a658536491fd3dcf74469329102cd789be42d262874b942f94**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "CHOOSE\_PRE\_INSTALLED\_MODEL\_KEY" : "CHOOSE\_PRE\_INSTALLED\_MODEL\_KEY"  |
| "CPU\_POWER\_MODE\_KEY" : "CPU\_POWER\_MODE\_KEY"  |
| "CPU\_THREAD\_NUM\_KEY" : "CPU\_THREAD\_NUM\_KEY"  |
| "DET\_LONG\_SIZE\_KEY" : "DET\_LONG\_SIZE\_KEY"  |
| "ENABLE\_CUSTOM\_SETTINGS\_KEY" : "ENABLE\_CUSTOM\_SETTINGS\_KEY"  |
| "IMAGE\_PATH\_KEY" : "IMAGE\_PATH\_KEY"  |
| "MODEL\_PATH\_KEY" : "MODEL\_PATH\_KEY"  |

## **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.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.MANAGE\_EXTERNAL\_STORAGE | 危险 | 允许应用程序广泛访问范围存储中的外部存储 | 允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.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.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.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.KILL\_BACKGROUND\_PROCESSES | 正常 | 杀死后台进程 | 允许应用程序杀死其他应用程序的后台进程,即使内存不低 |
| 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 |
| android.permission.GET\_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| com.android.greaderex.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。**