MoGua

福多多福袋助手 1.738.APK 分析报告

APP名称:	福多多福袋助手

包名:	com.android.greaderex
域名线索:	5条
URL线索:	6条
邮箱线索:	1条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

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

APP 信息

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

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 **纬度**: 37.266792 **经度**: 127.016335
update.xreader22.top	**IP**: 47.100.32.93 **所属国家**: China **地区**: Shanghai **城市**: Shanghai **纬度**: 31.224333 **经度**: 121.468948
v.douyin.com	**IP**: 119.167.184.232 **所属国家**: China **地区**: Shandong

	城市: Qingdao **纬度**: 36.098610 **经度**: 120.371941
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 **纬度**: 39.907501 **经度**: 116.397102

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

邮箱线索

邮箱地址	所在文件
hzxsgfzl@gmail.com	摸瓜V1引擎

手机线索

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

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"

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接

登陆摸瓜网站后查看		

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

应用内通信