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

**多多应急（ 4.1.2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 | 多多应急 |
| 版本 | 4.1.2 |
| 包名 | com.android.lixiangjinronh |
| 域名线索 | 43条 |
| URL线索 | 33条 |
| APP图标 |  |
| 分析日期 | 2025年6月26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 | com.android.lixiangjinronh.apk |
| 文件大小 | 19.1MB |
| MD5值 | 42e0a3f8b9edb34f768336cd2fe191bd |
| SHA1值 | 967dd843058f8b07b5b1f2b973b0b2569f9e1b3b |
| SHA256值 | 01ae37b46a9cee5907f122157eb7a3a2efa34ad42356fa117c095aed030546dc |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 多多应急 |
| 包名 | com.android.lixiangjinronh |
| 主活动Activity | com.duoduoyingjidf.ui.activitys.JDXF0ACT |
| 安卓版本名称 | 4.1.2 |
| 安卓版本 | 52 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| i.open.t.sina.com.cn | IP: 10.7.129.112 所属国家: - 地区: - 城市: -  |
| render.alipay.com | IP: 124.95.153.221 所属国家: China 地区: Liaoning 城市: Shenyang  |
| cloudauth-dualstack.aliyuncs.com | IP: 106.11.172.8 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com | IP: 140.206.110.66 所属国家: China 地区: Shanghai 城市: Shanghai  |
| plus.google.com | IP: 108.160.163.117 所属国家: United States of America 地区: California 城市: San Francisco  |
| c.y.qq.com | IP: 116.128.171.220 所属国家: China 地区: Shanghai 城市: Shanghai  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.youtube.com | IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco  |
| y.gtimg.cn | IP: 59.83.212.234 所属国家: China 地区: Jiangsu 城市: Wuxi  |
| music.163.com | IP: 220.197.30.65 所属国家: China 地区: Jiangsu 城市: Nanjing  |
| api.xiami.com | 没有服务器地理信息.  |
| cfg.imtt.qq.com | IP: 60.28.172.238 所属国家: China 地区: Tianjin 城市: Tianjin  |
| h.xiami.com | 没有服务器地理信息.  |
| pms.mb.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |
| www.beizhuabao.com | 没有服务器地理信息.  |
| service.weibo.com | IP: 123.125.107.14 所属国家: China 地区: Beijing 城市: Beijing  |
| open.weibo.cn | IP: 123.125.107.13 所属国家: China 地区: Beijing 城市: Beijing  |
| y.qq.com | IP: 58.144.243.128 所属国家: China 地区: Chongqing 城市: Chongqing  |
| pop.yuncloudauth.com | IP: 59.82.44.22 所属国家: China 地区: Shanghai 城市: Shanghai  |
| nice800.com | IP: 43.132.110.135 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| tianshu.alicdn.com | IP: 122.156.129.119 所属国家: China 地区: Heilongjiang 城市: Heihe  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| schemas.android.com | 没有服务器地理信息.  |
| cloudauth-dualstack.cn-beijing.aliyuncs.com | IP: 39.97.154.8 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| android.bugly.qq.com | IP: 124.95.225.169 所属国家: China 地区: Liaoning 城市: Shenyang  |
| mxncvjkhkaherwq.oss-accelerate.aliyuncs.com | IP: 39.107.134.21 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| android-donwload.oss-cn-hangzhou.aliyuncs.com | IP: 101.67.62.58 所属国家: China 地区: Zhejiang 城市: Huzhou  |
| accounts.google.com | IP: 173.194.203.84 所属国家: United States of America 地区: California 城市: Mountain View  |
| cloudauth.aliyuncs.com | IP: 59.82.44.22 所属国家: China 地区: Shanghai 城市: Shanghai  |
| acs.m.xiami.com | IP: 203.119.145.40 所属国家: China 地区: Beijing 城市: Beijing  |
| github.com | IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| u.y.qq.com | IP: 220.194.111.241 所属国家: China 地区: Tianjin 城市: Tianjin  |
| mgw.mpaas.cn-hangzhou.aliyuncs.com | IP: 47.118.168.189 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| auth.yunverify.com | IP: 59.82.44.22 所属国家: China 地区: Shanghai 城市: Shanghai  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com | IP: 36.248.13.185 所属国家: China 地区: Fujian 城市: Fuzhou  |
| feross.org | IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont  |
| cloudauth.cn-beijing.aliyuncs.com | IP: 39.97.154.134 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| www.xiami.com | IP: 59.82.31.244 所属国家: China 地区: Zhejiang 城市: Hangzhou  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | b/h/f/d/g.java  |
| https://mgw.mpaas.cn-hangzhou.aliyuncs.com  | com/alipay/alipaysecuritysdk/common/config/Configuration.java  |
| https://render.alipay.com/p/f/fd-j8l9yjja/index.html  | com/dtf/face/config/NavigatePage.java  |
| https://cloudauth-dualstack.aliyuncs.com  | com/dtf/face/api/DTFacadeExt.java  |
| https://cloudauth.aliyuncs.com  | com/dtf/face/api/DTFacadeExt.java  |
| https://cloudauth-dualstack.cn-beijing.aliyuncs.com  | com/dtf/face/api/DTFacadeExt.java  |
| https://cloudauth.cn-beijing.aliyuncs.com  | com/dtf/face/api/DTFacadeExt.java  |
| https://auth.yunverify.com  | com/dtf/face/api/DTFacadeExt.java  |
| https://pop.yuncloudauth.com  | com/dtf/face/api/DTFacadeExt.java  |
| http://xml.apache.org/xslt  | com/blankj/utilcode/util/LogUtils.java  |
| https://nice800.com  | com/duoduoyingjidf/ui/activitys/MT7ACT.java  |
| https://nice800.com/  | com/duoduoyingjidf/ui/activitys/MT10ACT.java  |
| http://debugtbs.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugx5.qq.com  | com/tencent/smtt/sdk/WebView.java  |
| http://debugtbs.qq.com?10000\  | com/tencent/smtt/sdk/WebView.java  |
| https://service.weibo.com/share/mobilesdk.php  | com/sina/weibo/sdk/web/WebActivity.java  |
| https://open.weibo.cn/oauth2/authorize?  | com/sina/weibo/sdk/web/WebActivity.java  |
| https://cn-shanghai-aliyun-cloudauth.oss-cn-shanghai.aliyuncs.com/model/toyger.face.dat  | d/h/a/n/k.java  |
| https://tianshu.alicdn.com/7504f3f0-aca8-4636-b486-e396559d3efb.png  | d/h/a/n/k.java  |
| https://android-donwload.oss-cn-hangzhou.aliyuncs.com/domai0dsfnName/5100sdfh0635.text/  | d/i/b/d/a/d.java  |
| https://mxncvjkhkaherwq.oss-accelerate.aliyuncs.com  | d/i/b/d/a/e.java  |
| https://ijljlkjzxcv-1324028813.cos.ap-guangzhou.myqcloud.com  | d/i/b/d/a/e.java  |
| https://jzlwjfanjzxcv.s3.ap-east-1.amazonaws.com  | d/i/b/d/a/e.java  |
| http://www.beizhuabao.com  | d/i/b/d/a/a.java  |
| http://www.beizhuabao.com  | d/i/b/d/a/b.java  |
| https://plus.google.com/  | d/l/a/c/c/k/s1.java  |
| https://accounts.google.com/o/oauth2/revoke?token=  | d/l/a/c/a/a/e/c/f.java  |
| http://schemas.android.com/apk/res-auto  | d/l/a/d/v/a.java  |
| http://www.youtube.com/watch?v=  | d/o/a/i/b/a.java  |
| https://www.youtube.com  | d/o/a/i/a/d/a.java  |
| https://www.youtube.com  | d/o/a/i/a/f/a.java  |
| https://service.weibo.com/share/mobilesdk.php  | d/r/a/a/i/c/d.java  |
| https://service.weibo.com/share/mobilesdk\_uppic.php  | d/r/a/a/a/d.java  |
| http://i.open.t.sina.com.cn/mobilesdk/sendmessage.php  | d/r/a/a/a/c.java  |
| https://android.bugly.qq.com/rqd/async  | d/s/a/d/a/b/a.java  |
| http://pms.mb.qq.com/rsp204  | d/s/b/b/w.java  |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u=  | d/s/b/b/p/e.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | d/s/b/c/w.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | d/s/b/c/w.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | d/s/b/c/w.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | d/s/b/c/w.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | d/s/b/c/w.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | d/s/b/c/m.java  |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/exceptions/OnErrorNotImplementedException.java  |
| https://render.alipay.com/p/yuyan/180020010001208736/aliyunFacewelcome.html  | 摸瓜V1引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://github.com/crypto-browserify/crypto-browserify  | 摸瓜V2引擎  |
| https://music.163.com/  | 摸瓜V2引擎  |
| http://music.163.com/discover  | 摸瓜V2引擎  |
| http://music.163.com  | 摸瓜V2引擎  |
| https://y.gtimg.cn/music/photo\_new/T002R300x300M000  | 摸瓜V2引擎  |
| https://y.qq.com/n/yqq/song/  | 摸瓜V2引擎  |
| http://y.gtimg.cn/music/photo\_new/T001R300x300M000  | 摸瓜V2引擎  |
| https://c.y.qq.com/v8/fcg-bin/fcg\_v8\_album\_info\_cp.fcg  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic/issues  | 摸瓜V2引擎  |
| https://github.com/indutny/elliptic  | 摸瓜V2引擎  |
| https://www.xiami.com/song/  | 摸瓜V2引擎  |
| https://c.y.qq.com  | 摸瓜V2引擎  |
| https://y.qq.com/portal/player.html  | 摸瓜V2引擎  |
| https://u.y.qq.com  | 摸瓜V2引擎  |
| http://acs.m.xiami.com/h5  | 摸瓜V2引擎  |
| http://api.xiami.com  | 摸瓜V2引擎  |
| http://h.xiami.com/  | 摸瓜V2引擎  |
| https://music.163.com  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0 u0013android@android.com  | d/l/a/c/c/v.java  |
| feross@feross.org git@github.com fedor@indutny.com  | 摸瓜V2引擎  |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 19919152923  | 摸瓜V2引擎  |

## **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=hslvkdkztkapk, ST=uppjmpsmthlsi, L=euaxvjukeaamv, O=ckt1747561005683, OU=dpp1747561005683, CN=TG@apken888 签名算法: rsassa\_pkcs1v15 有效期自: 2025-05-18 09:36:45+00:00 有效期至: 2075-05-06 09:36:45+00:00 发行人: C=hslvkdkztkapk, ST=uppjmpsmthlsi, L=euaxvjukeaamv, O=ckt1747561005683, OU=dpp1747561005683, CN=TG@apken888 序列号: 0xa1ab221 哈希算法: sha1 md5值: a24a5d7dd6a9b1bf9a6c7c153e6b09b0 sha1值: 17d19c27b96358cdfe8c6bcca4877f1f10550494 sha256值: 71ab5171de9889a058652818d71c8907785b55297474239198daee40a6f5d15d sha512值: 2be7f8dd57fca06546321e60ca211a732f6003450937951bc2a00eea2c6022decfc163df2e7cb75f62d82e99c62a0295ce87ba0ba3e99f565fe1d09528f4366b 公钥算法: rsa 密钥长度: 1024 指纹: 5a540b8a7b56e9f82e86db3a4aed49fe309aee1b164982c9e92ff9b47f7b8148**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "agreee\_user" : "请先同意并勾选用户协议"  |
| "check\_gesture\_pwd" : "验证手势密码"  |
| "check\_login\_pwd" : "验证登录密码"  |
| "dear\_user" : "尊敬的用户:"  |
| "find\_pwd" : "找回密码"  |
| "gesture\_pwd" : "手势密码"  |
| "has\_authd" : "已授权"  |
| "info\_auth\_fee" : "信息认证费 ："  |
| "info\_auth\_fee2" : "信息认证费"  |
| "input\_orgin\_pwd" : "请输入原密码"  |
| "input\_pwd" : "请输入验证码"  |
| "input\_pwd\_number" : "请输入新密码(6-16位数字字母组合)"  |
| "modify\_pwd" : "修改密码"  |
| "ple\_agree\_auth\_agreement" : "请先同意授权及借款协议"  |
| "ple\_input\_service\_pwd" : "请输入服务密码"  |
| "real\_auth" : "实名认证"  |
| "reset\_service\_pwd" : "重置服务密码"  |
| "service\_pwd" : "服务密码:"  |
| "to\_authorize" : "去授权"  |
| "user" : "用户"  |

## **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.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.CHANGE\_WIFI\_STATE | 正常 | 更改Wi-Fi状态 | 允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改 |
| 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.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.WRITE\_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| 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\_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.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.WRITE\_CALL\_LOG | 危险 |  | 允许应用程序写入（但不读取）用户号召日志数据。 |
| android.permission.READ\_CALL\_LOG | 危险 |  | 允许应用程序读取用户的通话日志 |
| 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.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.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.CHANGE\_NETWORK\_STATE | 正常 | 更改网络连接 | 允许应用程序更改网络连接状态。 |
| 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.READ\_MEDIA\_VISUAL\_USER\_SELECTED | 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 |
| android.permission.READ\_MEDIA\_AUDIO | 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。**