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

**广发基金（ 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 | 广发基金 |
| 版本 | 1.0.0 |
| 包名 | com.fdsfdsg164.fzf |
| 域名线索 | 14条 |
| URL线索 | 6条 |
| APP图标 |  |
| 分析日期 | 2025年6月17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 | Android.apk |
| 文件大小 | 8.15MB |
| MD5值 | 5190444ab9fd96ef1709cc8c29e59cf8 |
| SHA1值 | 428d068ba8d1ad5c4621e1ec4a6e104924e0857d |
| SHA256值 | 99702154d2bcdb5f5b4ebc108cdb25cd7aa94da1afe376cea0fc2a140c2ea268 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 广发基金 |
| 包名 | com.fdsfdsg164.fzf |
| 主活动Activity | com.uzmap.pkg.LauncherUI |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 1 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| log.tbs.qq.com | IP: 124.95.224.248 所属国家: China 地区: Liaoning 城市: Shenyang  |
| r.apicloud.com | 没有服务器地理信息.  |
| mdc.html5.qq.com | IP: 125.39.196.199 所属国家: China 地区: Tianjin 城市: Tianjin  |
| soft.tbs.imtt.qq.com | IP: 119.167.147.86 所属国家: China 地区: Shandong 城市: Qingdao  |
| wup.imtt.qq.com | IP: 125.39.196.183 所属国家: China 地区: Tianjin 城市: Tianjin  |
| d.apicloud.com | 没有服务器地理信息.  |
| as.apicloud.com | 没有服务器地理信息.  |
| p.apicloud.com | 没有服务器地理信息.  |
| debugx5.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| s.apicloud.com | 没有服务器地理信息.  |
| a.apicloud.com | 没有服务器地理信息.  |
| mqqad.html5.qq.com | IP: 0.0.0.1 所属国家: - 地区: - 城市: -  |
| debugtbs.qq.com | IP: 60.29.240.122 所属国家: China 地区: Tianjin 城市: Tianjin  |
| cfg.imtt.qq.com | IP: 60.29.240.17 所属国家: China 地区: Tianjin 城市: Tianjin  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| 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  |
| http://mdc.html5.qq.com/mh?channel\_id=50079&u=  | com/tencent/smtt/sdk/a/c.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11047  | com/tencent/smtt/sdk/b/a/a.java  |
| http://mdc.html5.qq.com/d/directdown.jsp?channel\_id=11041  | com/tencent/smtt/sdk/b/a/a.java  |
| http://log.tbs.qq.com/ajax?c=pu&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=pu&tk=  | com/tencent/smtt/utils/n.java  |
| http://wup.imtt.qq.com:8080  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=dl&k=  | com/tencent/smtt/utils/n.java  |
| http://cfg.imtt.qq.com/tbs?v=2&mk=  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ul&v=2&k=  | com/tencent/smtt/utils/n.java  |
| http://mqqad.html5.qq.com/adjs  | com/tencent/smtt/utils/n.java  |
| http://log.tbs.qq.com/ajax?c=ucfu&k=  | com/tencent/smtt/utils/n.java  |
| http://soft.tbs.imtt.qq.com/17421/tbs\_res\_imtt\_tbs\_DebugPlugin\_DebugPlugin.tbs  | com/tencent/smtt/utils/d.java  |
| https://a.apicloud.com  | compile/Properties.java  |
| https://d.apicloud.com  | compile/Properties.java  |
| https://s.apicloud.com  | compile/Properties.java  |
| https://p.apicloud.com  | compile/Properties.java  |
| https://r.apicloud.com  | compile/Properties.java  |
| https://as.apicloud.com  | compile/Properties.java  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| developer@apicloud.com  | com/uzmap/pkg/uzcore/b/d.java  |

### **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=(zh), ST=(Beijing), L=(Beijing), O=(1920991212@qq.com), OU=(fdsfdsg164), CN=(fdsfdsg164) 签名算法: rsassa\_pkcs1v15 有效期自: 2021-03-13 13:18:48+00:00 有效期至: 2121-02-17 13:18:48+00:00 发行人: C=(zh), ST=(Beijing), L=(Beijing), O=(1920991212@qq.com), OU=(fdsfdsg164), CN=(fdsfdsg164) 序列号: 0x28d4cef5 哈希算法: sha256 md5值: 5ad1595cb2c92356d79ab8c9035f4ec3 sha1值: 6d849753f118e8e1168879abd0fc60bc7f609cdc sha256值: c2a0bb60b90cdadae147367f3b463b625f903f21bda6c5ce0961a971eb160734 sha512值: e264110fc303c2e099999c02833d5fdce99afa06cbfca6529a37015143997703ebe4da59a8a1fb27a6acb7c6264a87dddf20d97042386449af45185bd84cefdc 公钥算法: rsa 密钥长度: 1024 指纹: 50ef1d36c6a5550f7562b7ed3911068135dbe1da901eca32f7903f4de77ea932**

## **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 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| 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.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.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.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.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.CALL\_PHONE | 危险 | 直接拨打电话号码 | 允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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。 |

## **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。**