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

**强国复兴（ 3.5.6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 | 强国复兴 |
| 版本 | 3.5.6 |
| 包名 | uni.ufxv |
| 域名线索 | 33条 |
| URL线索 | 21条 |
| APP图标 |  |
| 分析日期 | 2025年7月18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 | uni.ufxv.apk |
| 文件大小 | 27.25MB |
| MD5值 | de8f6885a63acd8fef505cd2a2e6b9eb |
| SHA1值 | 1c82b9814d9e4c7b340457b1123341fa8b105f17 |
| SHA256值 | 74ec9401db294b4e3a5224ea308a509d0327a2dc0a26dd6f7f44253669edca71 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 强国复兴 |
| 包名 | uni.ufxv |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 3.5.6 |
| 安卓版本 | 356 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| ask.dcloud.net.cn | IP: 39.91.140.106  所属国家: China  地区: Shandong  城市: Linyi |
| beijing-5.zos.ctyun.cn | IP: 49.7.99.37  所属国家: China  地区: Beijing  城市: Beijing |
| hjk.wndlw.com | 没有服务器地理信息. |
| fbb.nfmsbg.com | 没有服务器地理信息. |
| wwddyy64567.oss-rg-china-mainland.aliyuncs.com | IP: 39.101.36.167  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| fasdada.bj.bcebos.com | IP: 113.200.2.111  所属国家: China  地区: Shaanxi  城市: Yulin |
| dsadsadad.cn-bj.ufileos.com | IP: 117.50.123.23  所属国家: China  地区: Shanghai  城市: Shanghai |
| vasvavvv.bd.bcebos.com | IP: 110.242.70.8  所属国家: China  地区: Hebei  城市: Baoding |
| vxcvxvcv.oss-rg-china-mainland.aliyuncs.com | IP: 39.101.36.167  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| szszjsh6543.oss-cn-shenzhen.aliyuncs.com | IP: 112.74.1.211  所属国家: China  地区: Guangdong  城市: Shenzhen |
| obs-gzgy2.cucloud.cn | IP: 59.80.34.200  所属国家: China  地区: Guizhou  城市: Guiyang |
| apis.map.qq.com | IP: 116.130.223.114  所属国家: China  地区: Beijing  城市: Beijing |
| feqdwqdf.oss-rg-china-mainland.aliyuncs.com | IP: 39.101.36.167  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| quilljs.com | IP: 172.66.40.163  所属国家: United States of America  地区: California  城市: San Francisco |
| qwe.spnpw.com | 没有服务器地理信息. |
| obs-helf.cucloud.cn | IP: 120.52.92.249  所属国家: China  地区: Hebei  城市: Langfang |
| www.google.com | IP: 199.59.148.96  所属国家: United States of America  地区: California  城市: San Francisco |
| ns.adobe.com | 没有服务器地理信息. |
| er.dcloud.net.cn | IP: 43.142.57.168  所属国家: China  地区: Beijing  城市: Beijing |
| bjbjbjbjbjbjbjbjbjbj.oss-cn-beijing.aliyuncs.com | IP: 39.97.203.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| grefewwf.oss-cn-beijing.aliyuncs.com | IP: 39.97.203.30  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| service.dcloud.net.cn | IP: 111.229.199.57  所属国家: China  地区: Beijing  城市: Beijing |
| jiangsu-10.zos.ctyun.cn | IP: 117.88.33.247  所属国家: China  地区: Jiangsu  城市: Nanjing |
| asd.wndlw.com | 没有服务器地理信息. |
| fsadadad.tos-cn-beijing.volces.com | IP: 221.194.175.118  所属国家: China  地区: Hebei  城市: Langfang |
| er.dcloud.io | 没有服务器地理信息. |
| m3w.cn | IP: 42.236.84.33  所属国家: China  地区: Henan  城市: Zhengzhou |
| bnm.spnpw.com | 没有服务器地理信息. |
| dycecess.tos-cn-guangzhou.volces.com | IP: 157.255.228.134  所属国家: China  地区: Guangdong  城市: Shenzhen |
| dwc.nfmsbg.com | 没有服务器地理信息. |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| schemas.android.com | 没有服务器地理信息. |
| ukdosscs.cn-gd.ufileos.com | IP: 106.75.183.117  所属国家: China  地区: Shanghai  城市: Shanghai |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://ns.adobe.com/xap/1.0/\u0000 | io/dcloud/common/util/ExifInterface.java |
| https://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| https://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.java |
| https://er.dcloud.io/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://er.dcloud.net.cn/sc | io/dcloud/feature/gg/dcloud/ADHandler.java |
| https://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://ask.dcloud.net.cn/article/35627 | io/dcloud/e/b/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/e/b/a.java |
| https://er.dcloud.io/rv | io/dcloud/e/c/h/c.java |
| https://er.dcloud.net.cn/rv | io/dcloud/e/c/h/c.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/g/b.java |
| https://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextureView.java |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifTextView.java |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |
| https://apis.map.qq.com/jsapi?qt=translate&type=1&points= | 摸瓜V2引擎 |
| https://apis.map.qq.com/uri/v1/routeplan?type=drive&to= | 摸瓜V2引擎 |
| https://www.google.com/maps/?daddr= | 摸瓜V2引擎 |
| https://www.google.com/maps/ | 摸瓜V2引擎 |
| https://quilljs.com/ | 摸瓜V2引擎 |
| https://quilljs.com | 摸瓜V2引擎 |
| https://feqdwqdf.oss-rg-china-mainland.aliyuncs.com/0606dsadapi.txt | 摸瓜V2引擎 |
| https://grefewwf.oss-cn-beijing.aliyuncs.com/0606dsadapi.txt | 摸瓜V2引擎 |
| https://szszjsh6543.oss-cn-shenzhen.aliyuncs.com/jjqw8298cxbuapi.txt | 摸瓜V2引擎 |
| https://wwddyy64567.oss-rg-china-mainland.aliyuncs.com/jjqw8298cxbuapi.txt | 摸瓜V2引擎 |
| https://bjbjbjbjbjbjbjbjbjbj.oss-cn-beijing.aliyuncs.com/b1652sdfsapi.txt | 摸瓜V2引擎 |
| https://vxcvxvcv.oss-rg-china-mainland.aliyuncs.com/b1652sdfsapi.txt | 摸瓜V2引擎 |
| https://obs-helf.cucloud.cn/fasdsaddd/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://obs-gzgy2.cucloud.cn/fewfewfwfw/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://jiangsu-10.zos.ctyun.cn/bucket-36cf/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://beijing-5.zos.ctyun.cn/bucket-7fa3/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://fasdada.bj.bcebos.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://vasvavvv.bd.bcebos.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://ukdosscs.cn-gd.ufileos.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://dsadsadad.cn-bj.ufileos.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://dycecess.tos-cn-guangzhou.volces.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://fsadadad.tos-cn-beijing.volces.com/ukdcedsadapi.txt | 摸瓜V2引擎 |
| https://qwe.spnpw.com | 摸瓜V2引擎 |
| https://bnm.spnpw.com | 摸瓜V2引擎 |
| https://asd.wndlw.com | 摸瓜V2引擎 |
| https://hjk.wndlw.com | 摸瓜V2引擎 |
| https://dwc.nfmsbg.com | 摸瓜V2引擎 |
| https://fbb.nfmsbg.com | 摸瓜V2引擎 |
| https://service.dcloud.net.cn/uniapp/feedback.html | 摸瓜V2引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| jhruby.web@gmail.com | 摸瓜V2引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 17179869184 | tv/danmaku/ijk/media/player/IjkMediaMeta.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: True 找到 1 个唯一证书 主题: C=chengdu, ST=chengdu, L=chengdu, O=km1724281685380, OU=cr1724281685380, CN=bhsw 签名算法: rsassa\_pkcs1v15 有效期自: 2024-08-21 23:08:05+00:00 有效期至: 2074-08-09 23:08:05+00:00 发行人: C=chengdu, ST=chengdu, L=chengdu, O=km1724281685380, OU=cr1724281685380, CN=bhsw 序列号: 0xb13631 哈希算法: sha1 md5值: 74f8fbe6378f359592f2da6abec1bef3 sha1值: 433e9bf731ced06e57729e95fb778633dfb452a8 sha256值: 0a82ebf37ebb3c62d5293f981b0980c3b0e6fe424df47668b4a2caa3fde7c65d sha512值: 23b6c8c1e694842749e09bc5ddfaa4a7dccc8dadd399badee6deb3d0cede01b1d373359f89532ac9119827b31dd1d650f9f94f49462008bc47c4567b0455bb0e 公钥算法: rsa 密钥长度: 1024 指纹: 23596a436cea07409a77a31ee66efdd93ad22e1dd4242d596658bcfc16c4f914**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "dcloud\_common\_user\_refuse\_api" : "the user denies access to the API" |
| "dcloud\_io\_without\_authorization" : "not authorized" |
| "dcloud\_oauth\_authentication\_failed" : "failed to obtain authorization to log in to the authentication service" |
| "dcloud\_oauth\_empower\_failed" : "the Authentication Service operation to obtain authorized logon failed" |
| "dcloud\_oauth\_logout\_tips" : "not logged in or logged out" |
| "dcloud\_oauth\_oauth\_not\_empower" : "oAuth authorization has not been obtained" |
| "dcloud\_oauth\_token\_failed" : "failed to get token" |
| "dcloud\_permissions\_reauthorization" : "reauthorize" |
| "dcloud\_tips\_certificate" : "certificate" |
| "dcloud\_common\_user\_refuse\_api" : "用户拒绝该API访问" |
| "dcloud\_io\_without\_authorization" : "没有获得授权" |
| "dcloud\_oauth\_authentication\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_empower\_failed" : "获取授权登录认证服务操作失败" |
| "dcloud\_oauth\_logout\_tips" : "未登录或登录已注销" |
| "dcloud\_oauth\_oauth\_not\_empower" : "尚未获取oauth授权" |
| "dcloud\_oauth\_token\_failed" : "获取token失败" |
| "dcloud\_permissions\_reauthorization" : "重新授权" |
| "dcloud\_tips\_certificate" : "证书" |

## **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.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.INSTALL\_PACKAGES | 系统需要 | 直接安装应用程序 | 允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序 |
| 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.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.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.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.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.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\_VISUAL\_USER\_SELECTED | 未知 | Unknown permission | Unknown permission from android reference |
| 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。 |
| com.vivo.notification.permission.BADGE\_ICON | 未知 | Unknown permission | Unknown permission from android reference |
| com.asus.msa.SupplementaryDID.ACCESS | 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。**