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

**l灵宠链（ 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 | l灵宠链 |
| 版本 | 1.0.0 |
| 包名 | com.ilingchong.app |
| 域名线索 | 26条 |
| URL线索 | 25条 |
| APP图标 |  |
| 分析日期 | 2025年6月13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 | 灵宠链.apk |
| 文件大小 | 41.92MB |
| MD5值 | c838532c75b97c1d3607746a9666c912 |
| SHA1值 | cf994e8ee13d727d62624ed9a79c5bd76913db19 |
| SHA256值 | 6d83fa493664953973a5a0856d4dd395cf5d04d4a3157013cde0a82768d77113 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | l灵宠链 |
| 包名 | com.ilingchong.app |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 1.0.0 |
| 安卓版本 | 110 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.mescroll.com | IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| momentjs.com | IP: 104.16.32.155 所属国家: United States of America 地区: California 城市: San Francisco  |
| apis.map.qq.com | IP: 116.130.223.114 所属国家: China 地区: Beijing 城市: Beijing  |
| docs.goeasy.io | IP: 222.134.1.30 所属国家: China 地区: Shandong 城市: Binzhou  |
| uniapp.dcloud.net.cn | IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang  |
| at.alicdn.com | IP: 61.182.130.251 所属国家: China 地区: Hebei 城市: Zhangjiakou  |
| vkceyugu.cdn.bspapp.com | IP: 124.95.150.69 所属国家: China 地区: Liaoning 城市: Shenyang  |
| quilljs.com | IP: 172.66.43.93 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| feross.org | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| api.bspapp.com | IP: 39.96.249.142 所属国家: China 地区: Beijing 城市: Beijing  |
| game.gtimg.cn | IP: 115.56.90.216 所属国家: China 地区: Henan 城市: Jiaozuo  |
| 202.189.7.94 | IP: 202.189.7.94 所属国家: China 地区: Shandong 城市: Jinan  |
| m3w.cn | IP: 116.196.150.237 所属国家: China 地区: Zhejiang 城市: Jinhua  |
| service.dcloud.net.cn | IP: 110.40.169.99 所属国家: China 地区: Beijing 城市: Beijing  |
| imgcache.qq.com | IP: 123.138.255.10 所属国家: China 地区: Shaanxi 城市: Xi'an  |
| ns.adobe.com | 没有服务器地理信息.  |
| www.w3.org | IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco  |
| api.next.bspapp.com | IP: 203.107.60.33 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| er.dcloud.io | 没有服务器地理信息.  |
| ask.dcloud.net.cn | IP: 101.72.227.61 所属国家: China 地区: Hebei 城市: Langfang  |
| schemas.android.com | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| www.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| er.dcloud.net.cn | IP: 127.0.0.1 所属国家: - 地区: - 城市: -  |
| 103.91.209.118 | IP: 103.91.209.118 所属国家: China 地区: Shandong 城市: Jinan  |
| www.google.com | IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| http://schemas.android.com/apk/res/android  | com/hjq/permissions/AndroidManifestParser.java  |
| 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/283  | io/dcloud/feature/utsplugin/ProxyModule.java  |
| https://ask.dcloud.net.cn/article/35058  | io/dcloud/feature/audio/AudioRecorderMgr.java  |
| https://ask.dcloud.net.cn/article/35627  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/35877  | io/dcloud/p/r.java  |
| https://ask.dcloud.net.cn/article/283  | io/dcloud/p/h1.java  |
| https://er.dcloud.io/rv  | io/dcloud/p/d0.java  |
| https://er.dcloud.net.cn/rv  | io/dcloud/p/d0.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  |
| http://momentjs.com/guides/  | 摸瓜V2引擎  |
| http://feross.org>  | 摸瓜V2引擎  |
| https://vkceyugu.cdn.bspapp.com/VKCEYUGU-6bef1fe3-e3e3-4909-9f0c-6ed9bd11c93b/aae2360a-6628-4c93-b873-ce1600b9a852.apk  | 摸瓜V2引擎  |
| http://202.189.7.94/index/index/home?visiter\_id=  | 摸瓜V2引擎  |
| https://wx-  | 摸瓜V2引擎  |
| https://www.mescroll.com/img/mescroll-totop.png  | 摸瓜V2引擎  |
| https://www.mescroll.com/img/mescroll-empty.png  | 摸瓜V2引擎  |
| http://103.91.209.118:7777/zx534/  | 摸瓜V2引擎  |
| http://103.91.209.118:7777  | 摸瓜V2引擎  |
| https://api.next.bspapp.com  | 摸瓜V2引擎  |
| https://api.bspapp.com  | 摸瓜V2引擎  |
| https://uniapp.dcloud.net.cn/uniCloud/secure-network.html  | 摸瓜V2引擎  |
| https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise  | 摸瓜V2引擎  |
| https://github.com/facebook/regenerator/blob/main/LICENSE  | 摸瓜V2引擎  |
| https://feross.org/opensource>  | 摸瓜V2引擎  |
| https://github.com/ecomfe/zrender/blob/master/LICENSE.txt  | 摸瓜V2引擎  |
| https://imgcache.qq.com/open/qcloud/tim/assets/emoji/  | 摸瓜V2引擎  |
| https://docs.goeasy.io/2.x/im/message/media/alioss  | 摸瓜V2引擎  |
| https://at.alicdn.com/t/font\_2225171\_8kdcwk4po24.ttf)  | 摸瓜V2引擎  |
| https://game.gtimg.cn/images/mdnf/web202405/side\_yuyue\_light.png)  | 摸瓜V2引擎  |
| https://service.dcloud.net.cn/uniapp/feedback.html  | 摸瓜V2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  |
| http://www.apache.org/licenses/LICENSE-2.0  | 摸瓜V2引擎  |
| https://github.com/ecomfe/zrender/blob/master/LICENSE.txt  | 摸瓜V2引擎  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| emoji\_0@2x.png emoji\_1@2x.png emoji\_2@2x.png emoji\_3@2x.png emoji\_4@2x.png emoji\_5@2x.png emoji\_6@2x.png emoji\_7@2x.png emoji\_8@2x.png emoji\_9@2x.png emoji\_10@2x.png emoji\_11@2x.png emoji\_12@2x.png emoji\_13@2x.png emoji\_14@2x.png emoji\_15@2x.png emoji\_16@2x.png emoji\_17@2x.png emoji\_18@2x.png emoji\_19@2x.png emoji\_20@2x.png emoji\_21@2x.png emoji\_22@2x.png emoji\_23@2x.png emoji\_24@2x.png emoji\_25@2x.png emoji\_26@2x.png emoji\_27@2x.png emoji\_28@2x.png emoji\_29@2x.png emoji\_30@2x.png emoji\_31@2x.png emoji\_32@2x.png emoji\_33@2x.png emoji\_34@2x.png emoji\_35@2x.png emoji\_36@2x.png emoji\_37@2x.png emoji\_38@2x.png emoji\_39@2x.png emoji\_40@2x.png emoji\_41@2x.png emoji\_42@2x.png emoji\_43@2x.png emoji\_44@2x.png emoji\_45@2x.png emoji\_46@2x.png emoji\_47@2x.png emoji\_48@2x.png emoji\_49@2x.png emoji\_50@2x.png emoji\_51@2x.png emoji\_52@2x.png emoji\_53@2x.png emoji\_54@2x.png emoji\_55@2x.png emoji\_56@2x.png emoji\_57@2x.png emoji\_58@2x.png emoji\_59@2x.png emoji\_60@2x.png emoji\_61@2x.png emoji\_62@2x.png emoji\_63@2x.png emoji\_64@2x.png emoji\_65@2x.png emoji\_66@2x.png emoji\_67@2x.png emoji\_68@2x.png emoji\_69@2x.png emoji\_70@2x.png emoji\_71@2x.png emoji\_72@2x.png emoji\_73@2x.png emoji\_74@2x.png emoji\_75@2x.png emoji\_76@2x.png emoji\_77@2x.png emoji\_78@2x.png emoji\_79@2x.png emoji\_80@2x.png emoji\_81@2x.png emoji\_82@2x.png emoji\_83@2x.png emoji\_84@2x.png emoji\_85@2x.png emoji\_86@2x.png emoji\_87@2x.png emoji\_88@2x.png emoji\_89@2x.png emoji\_90@2x.png emoji\_91@2x.png emoji\_92@2x.png emoji\_93@2x.png emoji\_94@2x.png emoji\_95@2x.png emoji\_96@2x.png emoji\_97@2x.png emoji\_98@2x.png emoji\_99@2x.png emoji\_100@2x.png emoji\_101@2x.png emoji\_102@2x.png emoji\_103@2x.png emoji\_104@2x.png emoji\_105@2x.png emoji\_106@2x.png emoji\_107@2x.png emoji\_108@2x.png emoji\_109@2x.png emoji\_110@2x.png emoji\_111@2x.png emoji\_112@2x.png emoji\_113@2x.png emoji\_114@2x.png emoji\_115@2x.png emoji\_116@2x.png emoji\_117@2x.png emoji\_118@2x.png emoji\_119@2x.png emoji\_120@2x.png emoji\_121@2x.png emoji\_122@2x.png emoji\_123@2x.png emoji\_124@2x.png emoji\_125@2x.png emoji\_126@2x.png emoji\_127@2x.png emoji\_128@2x.png emoji\_129@2x.png emoji\_130@2x.png emoji\_131@2x.png emoji\_132@2x.png emoji\_133@2x.png emoji\_134@2x.png emoji\_135@2x.png emoji\_136@2x.png emoji\_137@2x.png emoji\_138@2x.png emoji\_139@2x.png emoji\_140@2x.png emoji\_141@2x.png  | 摸瓜V2引擎  |

### **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: True 找到 1 个唯一证书 主题: C=CN, ST=北京, L=北京, O=北京精灵宠链商贸有限公司, OU=北京精灵宠链商贸有限公司, CN=灵宠链 签名算法: rsassa\_pkcs1v15 有效期自: 2025-04-29 06:10:41+00:00 有效期至: 2125-04-05 06:10:41+00:00 发行人: C=CN, ST=北京, L=北京, O=北京精灵宠链商贸有限公司, OU=北京精灵宠链商贸有限公司, CN=灵宠链 序列号: 0x20629d96 哈希算法: sha256 md5值: 026c7f1e53f5caa56b674daa7e7e9edf sha1值: ac694b9f932835ea18128e10da38112eefd1cd51 sha256值: 5f0994829ff02382b531b687d077beba37ad4cf07e98dc1e63bc355ecd155ad7 sha512值: f279fbf66d47513e60a76ad784039e3dc0354efaec644588286ce64e3535a01985407ab9ce396caabca9bf4c0c432d12872797d274a5efd0cbf17dd9099aafd0 公钥算法: rsa 密钥长度: 2048 指纹: 6df376f552a3581db973ac830e0625aa762b6816e110f4f126402065e8f8aca1**

## **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.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\_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 |
| 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\_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 |
| 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 |
| 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 |
| com.ilingchong.app.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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.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.MOUNT\_UNMOUNT\_FILESYSTEMS | 危险 | 装载和卸载文件系统 | 允许应用程序为可移动存储安装和卸载文件系统 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| android.permission.READ\_LOGS | 危险 | 读取敏感日志数据 | 允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| 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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.WRITE\_SETTINGS | 危险 | 修改全局系统设置 | 允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。 |

## **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。**