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

**绿果（ 6.6.7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 | 绿果 |
| 版本 | 6.6.7 |
| 包名 | cc.lvpao.mm |
| 域名线索 | 46条 |
| URL线索 | 39条 |
| APP图标 |  |
| 分析日期 | 2025年7月9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 | base.apk |
| 文件大小 | 29.76MB |
| MD5值 | ef54d0129935e730b6dd44efb400d02d |
| SHA1值 | c9f3e7f80ae9386afae2d92711f489e59a814c21 |
| SHA256值 | ce813ddd4b83cca1e5a995e1fc5a77803fafe4495fe9603b3b39e7c1ffa17e43 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 绿果 |
| 包名 | cc.lvpao.mm |
| 主活动Activity | io.dcloud.PandoraEntry |
| 安卓版本名称 | 6.6.7 |
| 安卓版本 | 667 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| msg.cmpassport.com | IP: 112.33.111.188  所属国家: China  地区: Anhui  城市: Hefei |
| klink.volceapplog.com | IP: 221.204.64.143  所属国家: China  地区: Shanxi  城市: Taiyuan |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| id6.me | IP: 42.123.76.150  所属国家: China  地区: Beijing  城市: Beijing |
| loggw-exsdk.alipay.com | IP: 110.76.6.82  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| 34.92.248.34 | IP: 34.92.248.34  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| mobilegw.alipay.com | IP: 203.209.255.238  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| cdn-icons-png.flaticon.com | IP: 23.41.187.18  所属国家: Italy  地区: Lombardia  城市: Milan |
| ns.adobe.com | 没有服务器地理信息. |
| schemas.android.com | 没有服务器地理信息. |
| ask.dcloud.net.cn | IP: 123.125.244.28  所属国家: China  地区: Beijing  城市: Beijing |
| applog.snssdk.com | IP: 116.136.186.206  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| ncopl.cn | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| h5.m.taobao.com | IP: 61.240.144.197  所属国家: China  地区: Hebei  城市: Shijiazhuang |
| quilljs.com | IP: 172.66.40.163  所属国家: United States of America  地区: California  城市: San Francisco |
| m3w.cn | IP: 116.136.15.191  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| mobilegwpre.alipay.com | IP: 110.75.138.35  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| toblog-alink.ctobsnssdk.com | IP: 123.6.144.207  所属国家: China  地区: Henan  城市: Zhengzhou |
| rest.apizza.net | IP: 139.198.11.16  所属国家: China  地区: Beijing  城市: Beijing |
| toblog.ctobsnssdk.com | IP: 116.136.186.203  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| tobapplog.volceapplog.com | IP: 121.17.123.104  所属国家: China  地区: Hebei  城市: Hengshui |
| er.dcloud.io | 没有服务器地理信息. |
| mclient.alipay.com | IP: 116.142.235.203  所属国家: China  地区: Beijing  城市: Beijing |
| toblog.volceapplog.com | IP: 116.196.143.220  所属国家: China  地区: Zhejiang  城市: Jinhua |
| www.google.com | IP: 199.59.148.96  所属国家: United States of America  地区: California  城市: San Francisco |
| www.crafilab.com | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| er.dcloud.net.cn | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| 30vta9rl4g.apifox.cn | IP: 120.27.226.76  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| wappaygw.alipay.com | IP: 116.142.245.206  所属国家: China  地区: Beijing  城市: Beijing |
| tobapplog.ctobsnssdk.com | IP: 221.204.58.138  所属国家: China  地区: Shanxi  城市: Taiyuan |
| log-api.oceanengine.com | IP: 116.136.186.203  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| momentjs.com | IP: 104.17.63.214  所属国家: United States of America  地区: California  城市: San Francisco |
| service.dcloud.net.cn | IP: 111.229.199.57  所属国家: China  地区: Beijing  城市: Beijing |
| mcgw.alipay.com | IP: 116.142.245.206  所属国家: China  地区: Beijing  城市: Beijing |
| cdn.pixabay.com | IP: 172.64.147.160  所属国家: United States of America  地区: California  城市: San Francisco |
| mobilegw.alipaydev.com | IP: 110.75.132.131  所属国家: China  地区: Zhejiang  城市: Hangzhou |
| abtest.volceapplog.com | IP: 124.165.219.219  所属国家: China  地区: Shanxi  城市: Taiyuan |
| apis.map.qq.com | IP: 116.130.224.140  所属国家: China  地区: Beijing  城市: Beijing |
| log.snssdk.com | IP: 116.136.186.207  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| render.alipay.com | IP: 124.165.219.237  所属国家: China  地区: Shanxi  城市: Taiyuan |
| analytics.oceanengine.com | IP: 116.136.186.207  所属国家: China  地区: Nei Mongol  城市: Hohhot |
| ichannel.snssdk.com | IP: 42.236.86.169  所属国家: China  地区: Henan  城市: Zhengzhou |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| nisportal.10010.com | IP: 124.64.196.20  所属国家: China  地区: Beijing  城市: Beijing |
| alink.volceapplog.com | IP: 116.196.135.202  所属国家: China  地区: Zhejiang  城市: Jinhua |
| databyterangers.com.cn | 没有服务器地理信息. |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://mobilegwpre.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/apmobilesecuritysdk/b/a.java |
| https://render.alipay.com/p/s/i?scheme=%s | com/alipay/sdk/app/OpenAuthTask.java |
| https://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://wappaygw.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/service/rest.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/home/exterfaceAssign.htm | com/alipay/sdk/app/PayTask.java |
| https://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| http://mclient.alipay.com/cashier/mobilepay.htm | com/alipay/sdk/app/PayTask.java |
| https://mobilegw.alipay.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mobilegw.alipaydev.com/mgw.htm | com/alipay/sdk/m/l/a.java |
| https://mcgw.alipay.com/sdklog.do | com/alipay/sdk/m/l/a.java |
| https://loggw-exsdk.alipay.com/loggw/logUpload.do | com/alipay/sdk/m/l/a.java |
| https://wappaygw.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://mclient.alipay.com/home/exterfaceAssign.htm? | com/alipay/sdk/m/l/a.java |
| https://h5.m.taobao.com/mlapp/olist.html | com/alipay/sdk/m/m/a.java |
| https://nisportal.10010.com:9001/api | com/bytedance/ad/common/uaid/identity/ChinaUnicomUAIDFetcher.java |
| https://nisportal.10010.com:9001/api?appid=1554778161154 | com/bytedance/ad/common/uaid/identity/ChinaUnicomUAIDFetcher.java |
| https://msg.cmpassport.com/h5/getMobile | com/bytedance/ad/common/uaid/identity/ChinaMobileUAIDFetcher.java |
| https://id6.me/gw/preuniq.do | com/bytedance/ad/common/uaid/identity/ChinaTelecomUAIDFetcher.java |
| https://analytics.oceanengine.com/sdk/app/ | com/bytedance/ads/convert/utils/NetWorkUtils.java |
| https://analytics.oceanengine.com/sdk/app/ | com/bytedance/ads/convert/utils/EventReporterV2.java |
| https://analytics.oceanengine.com/sdk/app/ | com/bytedance/ads/convert/utils/EventReporter.java |
| https://log-api.oceanengine.com | com/bytedance/applog/UriConfig.java |
| https://log.snssdk.com/service/2/device\_register/ | com/bytedance/applog/util/UriConstants.java |
| https://log.snssdk.com/service/2/device\_update | com/bytedance/applog/util/UriConstants.java |
| https://ichannel.snssdk.com/service/2/app\_alert\_check/ | com/bytedance/applog/util/UriConstants.java |
| https://log.snssdk.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://applog.snssdk.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://log.snssdk.com/service/2/log\_settings/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog-alink.ctobsnssdk.com/service/2/attribution\_data | com/bytedance/applog/util/UriConstants.java |
| https://toblog-alink.ctobsnssdk.com/service/2/alink\_data | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/device\_register/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/device\_update | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/app\_alert\_check/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://tobapplog.ctobsnssdk.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/profile/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/log\_settings/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.ctobsnssdk.com/service/2/abtest\_config/ | com/bytedance/applog/util/UriConstants.java |
| https://klink.volceapplog.com/service/2/device\_register/ | com/bytedance/applog/util/UriConstants.java |
| https://klink.volceapplog.com/service/2/device\_update | com/bytedance/applog/util/UriConstants.java |
| https://klink.volceapplog.com/service/2/app\_alert\_check/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.volceapplog.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://tobapplog.volceapplog.com/service/2/app\_log/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.volceapplog.com/service/2/profile/ | com/bytedance/applog/util/UriConstants.java |
| https://toblog.volceapplog.com/service/2/log\_settings/ | com/bytedance/applog/util/UriConstants.java |
| https://abtest.volceapplog.com/service/2/abtest\_config/ | com/bytedance/applog/util/UriConstants.java |
| https://alink.volceapplog.com/service/2/attribution\_data | com/bytedance/applog/util/UriConstants.java |
| https://alink.volceapplog.com/service/2/alink\_data | com/bytedance/applog/util/UriConstants.java |
| https://databyterangers.com.cn | com/bytedance/bdtracker/s3.java |
| http://schemas.android.com/apk/res/android | com/hjq/permissions/AndroidManifestParser.java |
| https://ask.dcloud.net.cn/article/35627 | b/a.java |
| https://ask.dcloud.net.cn/article/35877 | b/a.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://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |
| https://ask.dcloud.net.cn/article/283 | io/dcloud/feature/utsplugin/ProxyModule.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/287 | io/dcloud/share/IFShareApi.java |
| https://er.dcloud.io/rv | d/c.java |
| https://er.dcloud.net.cn/rv | d/c.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/283 | j/b.java |
| https://ask.dcloud.net.cn/article/36199 | 摸瓜V1引擎 |
| https://ncopl.cn/do/articleName\_h?name= | 摸瓜V2引擎 |
| https://ncopl.cn/do/ | 摸瓜V2引擎 |
| https://30vta9rl4g.apifox.cn | 摸瓜V2引擎 |
| http://34.92.248.34:8556 | 摸瓜V2引擎 |
| https://rest.apizza.net/rest/v2/Api/get\_history\_list?project\_id=5c556e7c41cd41a3b0f9b3b8e777ff2e | 摸瓜V2引擎 |
| https://cdn.pixabay.com/photo/2021/01/04/07/38/lily-5886728\_\_340.jpg | 摸瓜V2引擎 |
| https://github.com/facebook/regenerator/blob/main/LICENSE | 摸瓜V2引擎 |
| https://www.crafilab.com/ | 摸瓜V2引擎 |
| http://momentjs.com/guides/ | 摸瓜V2引擎 |
| https://github.com/emn178/js-md5 | 摸瓜V2引擎 |
| https://cdn-icons-png.flaticon.com/512/3406/3406954.png | 摸瓜V2引擎 |
| https://cdn-icons-png.flaticon.com/512/3406/3406874.png | 摸瓜V2引擎 |
| https://cdn-icons-png.flaticon.com/512/5058/5058432.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 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| emn178@gmail.com | 摸瓜V2引擎 |
| gold@2x.png  gold@3x.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=, L=, O=Android, OU=Android, CN=4NL1yYHFNwOG7o%2FqtMCNTEHUmItdnFZx5AQ7li7ETZeWthMhOZ6avcrTIo4Xkw%2ByQo1YH0wl818jyE0U%2Fy1XRw%3D%3D 签名算法: rsassa\_pkcs1v15 有效期自: 2025-03-21 03:46:09+00:00 有效期至: 2125-02-25 03:46:09+00:00 发行人: C=CN, ST=, L=, O=Android, OU=Android, CN=4NL1yYHFNwOG7o%2FqtMCNTEHUmItdnFZx5AQ7li7ETZeWthMhOZ6avcrTIo4Xkw%2ByQo1YH0wl818jyE0U%2Fy1XRw%3D%3D 序列号: 0x338f27e3 哈希算法: sha256 md5值: c6212c3ad66a249955ea302ffc142004 sha1值: 2ed62282cf862343c62cf8084662e84cb8a7eb7c sha256值: c945657727f774ef5ab61c3906c6b574ac5a3f5ea857ec2bc5494223958dc6ef sha512值: bd7e83f862f44818ceec4c92688b8ac5c1b6712795f9b2d53eed8c926e0a5651f86fcb38425494bf721f2c67d81fc47399856b6cd511aeb9bdf2012d1460a5e3 公钥算法: rsa 密钥长度: 2048 指纹: 056ab6500041dc55d19293e60bc55ab14b5b4e015e424f119ce9727634537387**

## **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.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\_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.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.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.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.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。**