



# MoGua

## 捷通 1.0.0.APK 分析报告



APP名称:

捷通

|        |                            |
|--------|----------------------------|
| 包名:    | nAeuequB.jsoarh.bwzkgurs   |
| 域名线索:  | 17条                        |
| URL线索: | 23条                        |
| 邮箱线索:  | 1条                         |
| 分析日期:  | 2025年6月26日                 |
| 分析平台:  | <a href="#">摸瓜APK反编译平台</a> |

文件名: 0624.apk  
文件大小: 12.94MB  
MD5值: 1269962a0bb76cb0100b59e9ad77b1c0  
SHA1值: f9e1b3dd3d36b5cc6e91934a5396e7f26a77b5d7  
SHA256值: e48848cad7ef6cc78cbb0f03437eabb7df758ee4048b86cd699ed75cec7a48fc

## i APP 信息

App名称: 捷通  
包名: nAeuequB.jsoarh.bwzkgurs  
主活动Activity: io.dcloud.PandoraEntry  
安卓版本名称: 1.0.0  
安卓版本: 100

## 🔍 域名线索

| 域名                  | 服务器信息                                                                                               |
|---------------------|-----------------------------------------------------------------------------------------------------|
| apis.map.qq.com     | IP: 116.130.223.114<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102 |
| schemas.android.com | 没有服务器地理信息.                                                                                          |
| ask.dcloud.net.cn   | IP: 123.12.235.54<br>所属国家: China<br>地区: Henan<br>城市: Hebi<br>纬度: 35.899170<br>经度: 114.192497        |
|                     |                                                                                                     |

|                       |                                                                                                                               |
|-----------------------|-------------------------------------------------------------------------------------------------------------------------------|
| www.google.com        | IP: 31.13.73.9<br>所属国家: Ireland<br>地区: Dublin<br>城市: Dublin<br>纬度: 53.344151<br>经度: -6.267249                                 |
| github.com            | IP: 20.205.243.166<br>所属国家: Singapore<br>地区: Singapore<br>城市: Singapore<br>纬度: 1.289987<br>经度: 103.850281                     |
| m3w.cn                | IP: 221.204.14.66<br>所属国家: China<br>地区: Shanxi<br>城市: Taiyuan<br>纬度: 37.869438<br>经度: 112.561508                              |
| service.dcloud.net.cn | IP: 111.229.199.57<br>所属国家: China<br>地区: Beijing<br>城市: Beijing<br>纬度: 39.907501<br>经度: 116.397102                            |
| er.dcloud.io          | 没有服务器地理信息.                                                                                                                    |
| ns.adobe.com          | 没有服务器地理信息.                                                                                                                    |
| www.w3.org            | IP: 104.18.22.19<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
|                       |                                                                                                                               |

|                  |                                                                                                                                |
|------------------|--------------------------------------------------------------------------------------------------------------------------------|
| lame.sf.net      | IP: 104.18.21.237<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| er.dcloud.net.cn | IP: 127.0.0.1<br>所属国家: -<br>地区: -<br>城市: -<br>纬度: 0.000000<br>经度: 0.000000                                                     |
| app.ysdll.com    | 没有服务器地理信息.                                                                                                                     |
| at.alicdn.com    | IP: 101.72.238.65<br>所属国家: China<br>地区: Hebei<br>城市: Langfang<br>纬度: 39.509720<br>经度: 116.694717                               |
| dk.rctcl.com     | 没有服务器地理信息.                                                                                                                     |
| quilljs.com      | IP: 172.66.40.163<br>所属国家: United States of America<br>地区: California<br>城市: San Francisco<br>纬度: 37.775700<br>经度: -122.395203 |
| feross.org       | IP: 50.116.11.184<br>所属国家: United States of America<br>地区: California<br>城市: Fremont<br>纬度: 37.548271<br>经度: -121.988571       |

## URL线索

| URL信息                                                                                               | Url所在文件                                       |
|-----------------------------------------------------------------------------------------------------|-----------------------------------------------|
| <a href="http://ns.adobe.com/xap/1.0/\u0000">http://ns.adobe.com/xap/1.0/\u0000</a>                 | io/dcloud/common/util/ExifInterface.java      |
| <a href="https://m3w.cn/s/">https://m3w.cn/s/</a>                                                   | io/dcloud/common/util/ShortCutUtil.java       |
| <a href="https://ask.dcloud.net.cn/article/282">https://ask.dcloud.net.cn/article/282</a>           | io/dcloud/common/constant/DOMException.java   |
| <a href="https://ask.dcloud.net.cn/article/35627">https://ask.dcloud.net.cn/article/35627</a>       | io/dcloud/e/b/a.java                          |
| <a href="https://ask.dcloud.net.cn/article/35877">https://ask.dcloud.net.cn/article/35877</a>       | io/dcloud/e/b/a.java                          |
| <a href="https://er.dcloud.io/rv">https://er.dcloud.io/rv</a>                                       | io/dcloud/e/c/h/c.java                        |
| <a href="https://er.dcloud.net.cn/rv">https://er.dcloud.net.cn/rv</a>                               | io/dcloud/e/c/h/c.java                        |
| <a href="https://er.dcloud.io/sc">https://er.dcloud.io/sc</a>                                       | io/dcloud/feature/gg/dcloud/ADHandler.java    |
| <a href="https://er.dcloud.net.cn/sc">https://er.dcloud.net.cn/sc</a>                               | io/dcloud/feature/gg/dcloud/ADHandler.java    |
| <a href="https://ask.dcloud.net.cn/article/35058">https://ask.dcloud.net.cn/article/35058</a>       | io/dcloud/feature/audio/AudioRecorderMgr.java |
| <a href="https://ask.dcloud.net.cn/article/283">https://ask.dcloud.net.cn/article/283</a>           | io/dcloud/g/b.java                            |
| <a href="https://ask.dcloud.net.cn/article/287">https://ask.dcloud.net.cn/article/287</a>           | io/dcloud/share/IFShareApi.java               |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a> | pl/droidsonroids/gif/GifViewUtils.java        |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a> | pl/droidsonroids/gif/GifTextureView.java      |
| <a href="http://schemas.android.com/apk/res/android">http://schemas.android.com/apk/res/android</a> | pl/droidsonroids/gif/GifTextView.java         |

|                                                                                                                                                   |                             |
|---------------------------------------------------------------------------------------------------------------------------------------------------|-----------------------------|
| <a href="https://ask.dcloud.net.cn/article/36199">https://ask.dcloud.net.cn/article/36199</a>                                                     | 摸瓜V1引擎                      |
| <a href="https://service.dcloud.net.cn/uniapp/feedback.html">https://service.dcloud.net.cn/uniapp/feedback.html</a>                               | 摸瓜V2引擎                      |
| <a href="https://apis.map.qq.com/jsapi?qt=translate&amp;type=1&amp;points=">https://apis.map.qq.com/jsapi?qt=translate&amp;type=1&amp;points=</a> | 摸瓜V2引擎                      |
| <a href="http://dk.rctcl.com/api/common/upload">http://dk.rctcl.com/api/common/upload</a>                                                         | 摸瓜V2引擎                      |
| <a href="https://github.com/facebook/regenerator/blob/main/LICENSE">https://github.com/facebook/regenerator/blob/main/LICENSE</a>                 | 摸瓜V2引擎                      |
| <a href="https://feross.org/opensource">https://feross.org/opensource</a> >                                                                       | 摸瓜V2引擎                      |
| <a href="https://app.ysdll.com/">https://app.ysdll.com/</a>                                                                                       | 摸瓜V2引擎                      |
| <a href="http://feross.org">http://feross.org</a> >                                                                                               | 摸瓜V2引擎                      |
| <a href="https://quilljs.com/">https://quilljs.com/</a>                                                                                           | 摸瓜V2引擎                      |
| <a href="https://quilljs.com">https://quilljs.com</a>                                                                                             | 摸瓜V2引擎                      |
| <a href="https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf">https://at.alicdn.com/t/font_2225171_8kdcwk4po24.ttf</a> )                         | 摸瓜V2引擎                      |
| <a href="https://apis.map.qq.com/uri/v1/routeplan?type=drive&amp;to=">https://apis.map.qq.com/uri/v1/routeplan?type=drive&amp;to=</a>             | 摸瓜V2引擎                      |
| <a href="https://www.google.com/maps/?daddr=">https://www.google.com/maps/?daddr=</a>                                                             | 摸瓜V2引擎                      |
| <a href="https://www.google.com/maps/">https://www.google.com/maps/</a>                                                                           | 摸瓜V2引擎                      |
| <a href="http://lame.sf.net">http://lame.sf.net</a>                                                                                               | lib/arm64-v8a/liblamemp3.so |

 邮箱线索

|  |  |
|--|--|
|  |  |
|--|--|

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

## 手机线索

## 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=rhFHZhhK, ST=WrsAuPJg, L=sOIUEJqO, O=swVtpybd, OU=SqNyHpKY, CN=DjsNwpAX  
签名算法: rsassa\_pkcs1v15  
有效期自: 2025-01-05 04:53:46+00:00  
有效期至: 2035-01-03 04:53:46+00:00  
发行人: C=rhFHZhhK, ST=WrsAuPJg, L=sOIUEJqO, O=swVtpybd, OU=SqNyHpKY, CN=DjsNwpAX  
序列号: 0xf3ce37ea15bec702  
哈希算法: sha256  
md5值: d162011906c5e7784c9fad843fc7e01c  
sha1值: ab582c99165a426027c1f363e80ffab003593447  
sha256值: b126aa741a7c9ae82aa0e0c5264ab82e7a0db26da34ef70262c1c085db188889  
sha512值: b2485a46f5bdabede46879c24bc1de1c3ff8c15e55a21980f071ef8b00d0a27fdf17eeb3c85119963e3264f374f2e268c9432a4117774d1ff848019982986aae  
公钥算法: rsa  
密钥长度: 2048  
指纹: e98dbca5cd01065476d5bd0e3eb6dafcdbcb11a4c3d9ad158122cd8720269fcb6

## 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"                                                                                |

加壳分析

| 加壳类型      | 所属文件 |
|-----------|------|
| 登陆摸瓜网站后查看 |      |

第三方插件

| 名称        | 分类 | URL链接 |
|-----------|----|-------|
| 登陆摸瓜网站后查看 |    |       |

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.FLASHLIGHT                | 正常   | 控制手电筒        | 允许应用程序控制手电筒                                                   |
| 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.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。这使它能够提供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.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.VIBRATE                   | 正    | 可控震源         | 允许应用程序控制振动器                                                   |

|                                                                                   |    |                    |                                           |
|-----------------------------------------------------------------------------------|----|--------------------|-------------------------------------------|
|                                                                                   | 常  |                    |                                           |
| 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.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。          |
| 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                             |
| nAeuequB.hHrhegrb.JojjpbgkmEf_com.asus.msa.SupplementaryDID.ACCESS                | 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_VISUAL_USER_SELECTED                                | 未知 | Unknown permission | Unknown permission from android reference |
| nAeuequB.hHrhegrb.JojjpbgkmEf_com.huawei.android.launcher.permission.CHANGE_BADGE | 未知 | Unknown permission | Unknown permission from android reference |
| nAeuequB.hHrhegrb.JojjpbgkmEf_com.vivo.notification.permission.BADGE_ICON         | 未知 | Unknown permission | Unknown permission from android reference |

应用内通信