MoGua

# APP线索分析报告

报告由 摸瓜APP分析平台(mogua.co) 生成


惠批零 1.0.APK

| | |
|---|---|
| APP名称: | 惠批零 |
| 包名: | w2a.W2Awww.huipiling.com |
| 域名线索: | 46条 |
| URL线索: | 44条 |
| 邮箱线索: | 0条 |
| 分析日期: | 2022年1月22日 17:51 |

## 文件信息

文件名: huipilian.apk
文件大小: 4.87MB
**MD5值:** 7856b7f2cb028a3438f08f08644a8b61
**SHA1值:** ae3b352c9ea129f0270f0e5da521cafd7e18cb2a
**SHA256值:** c220f9d0f348d12ed6532ff7571f674c69ec61a06a4fe1aba658ec4fe23019ab

# APP 信息

**App名称:** 惠批零
包名: w2a.W2Awww.huipiling.com
主活动**Activity:** io.dcloud.PandoraEntry
安卓版本名称: 1.0
安卓版本: 8

# 域名线索

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| www.huipiling.com.r.attr.fontstyle | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontproviderauthority | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontweight | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttontitlebackground | good | 没有服务器地理信息. |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| www.dcloud.io | good | **IP:** 124.239.227.205<br>**所属国家:** China<br>**地区:** Hebei<br>**城市:** Langfang<br>**纬度:** 39.509720<br>**经度:** 116.694717<br>**查看地图:** Google Map |
| schemas.android.com | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttonsinglebackground | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.destructivebuttontextcolor | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttonbottombackground | good | 没有服务器地理信息. |
| stream.mobihtml5.com | good | 没有服务器地理信息. |
| ask.dcloud.net.cn | good | **IP:** 124.239.227.208<br>**所属国家:** China<br>**地区:** Hebei<br>**城市:** Langfang<br>**纬度:** 39.509720<br>**经度:** 116.694717<br>**查看地图:** Google Map |
| www.huipiling.com.r.attr.gifsrc | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.titlebuttontextcolor | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.playcount | good | 没有服务器地理信息. |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| www.huipiling.com | good | **IP:** 154.220.40.181<br>**所属国家:** Hong Kong<br>**地区:** Hong Kong<br>**城市:** Hong Kong<br>**纬度:** 22.285521<br>**经度:** 114.157692<br>**查看地图:** Google Map |
| www.huipiling.com.r.attr.font | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.isopaque | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.freezesanimation | good | 没有服务器地理信息. |
| www.huipiling.com.wxapi | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.actionsheetstyle | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttontopbackground | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontprovidercerts | good | 没有服务器地理信息. |
| stream.dcloud.net.cn | good | **IP:** 118.31.103.188<br>**所属国家:** China<br>**地区:** Zhejiang<br>**城市:** Hangzhou<br>**纬度:** 30.293650<br>**经度:** 120.161423<br>**查看地图:** Google Map |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| m3w.cn | good | **IP:** 124.239.227.208<br>**所属国家:** China<br>**地区:** Hebei<br>**城市:** Langfang<br>**纬度:** 39.509720<br>**经度:** 116.694717<br>**查看地图:** Google Map |
| www.huipiling.com.r.attr.cancelbuttonbackground | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttonmiddlebackground | good | 没有服务器地理信息. |
| long.open.weixin.qq.com | good | **IP:** 109.244.217.35<br>**所属国家:** China<br>**地区:** Beijing<br>**城市:** Beijing<br>**纬度:** 39.907501<br>**经度:** 116.397232<br>**查看地图:** Google Map |
| api.weixin.qq.com | good | **IP:** 81.69.216.43<br>**所属国家:** China<br>**地区:** Beijing<br>**城市:** Beijing<br>**纬度:** 39.907501<br>**经度:** 116.397232<br>**查看地图:** Google Map |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| open.weixin.qq.com | good | **IP:** 175.24.209.30<br>**所属国家:** China<br>**地区:** Beijing<br>**城市:** Beijing<br>**纬度:** 39.907501<br>**经度:** 116.397232<br>**查看地图:** Google Map |
| www.huipiling.com.r.attr.actionsheetpadding | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontproviderfetchtimeout | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.actionsheettextsize | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.cancelbuttonmargintop | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontproviderquery | good | 没有服务器地理信息. |
| streamapp.sinaapp.com | good | **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<br>**查看地图:** Google Map |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| update.dcloud.net.cn | good | **IP:** 121.51.175.120<br>**所属国家:** China<br>**地区:** Guangdong<br>**城市:** Shenzhen<br>**纬度:** 22.545540<br>**经度:** 114.068298<br>**查看地图:** Google Map |
| www.huipiling.com.r.attr.loopcount | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.authplay | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontproviderfetchstrategy | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.cancelbuttontextcolor | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttontextcolor | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.otherbuttonspacing | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.gifsource | good | 没有服务器地理信息. |
| www.huipiling.com.r.attr.fontproviderpackage | good | 没有服务器地理信息. |
| service.dcloud.net.cn | good | **IP:** 47.97.36.120<br>**所属国家:** China<br>**地区:** Zhejiang<br>**城市:** Hangzhou<br>**纬度:** 30.293650<br>**经度:** 120.161423<br>**查看地图:** Google Map |

| 域名 | 是否危险域名 | 服务器信息 |
| --- | --- | --- |
| www.huipiling.com.r.attr.actionsheetbackground | good | 没有服务器地理信息. |

## URL线索

| URL信息 | Url所在文件 |
| --- | --- |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s | com/tencent/mm/opensdk/diffdev/a/f.java |
| https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s | com/tencent/mm/opensdk/diffdev/a/d.java |
| www.huipiling.com.R.attr.fontProviderAuthority, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontProviderCerts, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontProviderFetchStrategy, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontProviderFetchTimeout, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontProviderPackage, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontProviderQuery}; | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.font, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontStyle, | com/bumptech/glide/R.java |
| www.huipiling.com.R.attr.fontWeight}; | com/bumptech/glide/R.java |

| URL信息 | Url所在文件 |
| --- | --- |
| www.huipiling.com.R.attr.gifSource, | pl/droidsonroids/gif/R.java |
| www.huipiling.com.R.attr.isOpaque}; | pl/droidsonroids/gif/R.java |
| www.huipiling.com.R.attr.freezesAnimation, | pl/droidsonroids/gif/R.java |
| www.huipiling.com.R.attr.loopCount}; | pl/droidsonroids/gif/R.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 |
| http://schemas.android.com/apk/res/android | pl/droidsonroids/gif/GifViewUtils.java |
| www.huipiling.com.R.attr.actionSheetBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.actionSheetPadding, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.actionSheetTextSize, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.cancelButtonBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.cancelButtonMarginTop, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.cancelButtonTextColor, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.destructiveButtonTextColor, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonBottomBackground, | io/dcloud/base/R.java |

| URL信息 | Url所在文件 |
| --- | --- |
| www.huipiling.com.R.attr.otherButtonMiddleBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonSingleBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonSpacing, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonTextColor, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonTitleBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.otherButtonTopBackground, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.titleButtonTextColor}; | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.actionSheetStyle}; | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.authPlay, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.gifSrc, | io/dcloud/base/R.java |
| www.huipiling.com.R.attr.playCount}; | io/dcloud/base/R.java |
| http://m3w.cn/sd/reg | io/dcloud/appstream/b.java |
| http://m3w.cn/s/ | io/dcloud/appstream/c/b.java |
| http://ask.dcloud.net.cn/article/283 | io/dcloud/feature/b.java |
| http://ask.dcloud.net.cn/article/35058 | io/dcloud/feature/audio/AudioRecorderMgr.java |

| URL信息 | Url所在文件 |
| --- | --- |
| https://service.dcloud.net.cn/advert/splash | io/dcloud/feature/ad/a/a.java |
| https://api.weixin.qq.com/sns/auth?access_token=%s&openid=%s | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java |
| https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java |
| https://api.weixin.qq.com/sns/userinfo?access_token=%s&openid=%s&lang=zh_CN | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java |
| https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=%s&grant_type=refresh_token&refresh_token=%s | io/dcloud/feature/oauth/weixin/WeiXinOAuthService.java |
| http://ask.dcloud.net.cn/article/287 | io/dcloud/share/IFShareApi.java |
| https://service.dcloud.net.cn/collect/plusapp/action? | io/dcloud/common/util/TestUtil.java |
| http://m3w.cn/s/ | io/dcloud/common/util/ShortCutUtil.java |
| http://www.dcloud.io/streamapp/streamapp.apk | io/dcloud/common/util/ShortCutUtil.java |
| http://stream.dcloud.net.cn/resource/sitemap/v2?appid= | io/dcloud/common/a/d.java |
| https://service.dcloud.net.cn/collect/plusapp/startup | io/dcloud/common/a/d.java |
| http://ask.dcloud.net.cn/article/35627 | io/dcloud/common/a/a.java |
| https://ask.dcloud.net.cn/article/35877 | io/dcloud/common/a/a.java |
| https://service.dcloud.net.cn/sta/so?p=a&pn=%s&ver=%s&appid=%s | io/dcloud/common/core/a.java |
| http://ask.dcloud.net.cn/article/282 | io/dcloud/common/constant/DOMException.java |

| URL信息 | Url所在文件 |
| --- | --- |
| https://stream.mobihtml5.com/ | io/dcloud/common/constant/StringConst.java |
| https://stream.dcloud.net.cn/ | io/dcloud/common/constant/StringConst.java |
| http://update.dcloud.net.cn/apps/ | io/dcloud/common/constant/IntentConst.java |
| http://streamapp.sinaapp.com | io/dcloud/streamdownload/utils/b.java |
| www.huipiling.com; | w2a/W2Awww/huipiling/com/BuildConfig.java |
| www.huipiling.com | w2a/W2Awww/huipiling/com/BuildConfig.java |
| www.huipiling.com; | w2a/W2Awww/huipiling/com/R.java |
| www.huipiling.com.wxapi; | w2a/W2Awww/huipiling/com/wxapi/WXEntryActivity.java |

## 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 |

| 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.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.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.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.GET_TASKS | 危险 | 检索正在运行的应用程序 | 允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息 |
| android.permission.ACCESS_COARSE_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS_FINE_LOCATION | 危险 | 精细定位（GPS） | 访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量 |
| 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.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 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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.GET_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.MODIFY_AUDIO_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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_CONTACTS | 危险 | 读取联系人数据 | 允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人 |
| 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.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.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 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.RECORD_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.SYSTEM_ALERT_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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_CONTACTS | 危险 | 写入联系人数据 | 允许应用程序修改您手机上存储的联系人（地址）数据。恶意应用程序可以使用它来删除或修改您的联系人数据 |
| 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.RECEIVE_SMS | 危险 | 接收短信 | 允许应用程序接收和处理 SMS 消息。恶意应用程序可能会监视您的消息或将其删除而不向您显示 |
| android.permission.SEND_SMS | 危险 | 发送短信 | 允许应用程序发送 SMS 消息。恶意应用程序可能会在未经您确认的情况下发送消息,从而使您付出代价 |
| android.permission.WRITE_SMS | 危险 | 编辑短信或彩信 | 允许应用程序写入存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会删除您的消息 |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| android.permission.READ_SMS | 危险 | 阅读短信或彩信 | 允许应用程序读取存储在您的手机或 SIM 卡上的 SMS 消息。恶意应用程序可能会读取您的机密信息 |
| com.android.launcher.permission.UNINSTALL_SHORTCUT | 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.android.launcher.permission.INSTALL_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher2.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.launcher3.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.yulong.android.launcherL.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.meizu.flyme.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.bbk.launcher2.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.oppo.launcher.permission.READ_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.qiku.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.android.launcher.permission.READ_SETTINGS | 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.zte.mifavor.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.lenovo.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.yulong.android.launcher3.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| org.adw.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.qihoo360.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.lge.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| net.qihoo.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| org.adwfreak.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| org.adw.launcher_donut.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher3.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.fede.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.app.twlauncher.settings.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| com.tencent.qqlauncher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.huawei.launcher2.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.ebproductions.android.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.nd.android.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.yulong.android.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.android.mylauncher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.ztemt.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| cn.nubia.launcher.permission.READ_SETTINGS | 未知 | Unknown permission | Unknown permission from android reference |
| com.gionee.amisystem.permission.READ_SHORTCUT | 未知 | Unknown permission | Unknown permission from android reference |

| 向手机申请的权限 | 是否危险 | 类型 | 详细情况 |
| --- | --- | --- | --- |
| 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.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 |
| com.asus.msa.SupplementaryDID.ACCESS | 未知 | Unknown permission | Unknown permission from android reference |

# 签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=china, ST=henan, L=luoyang, O=tianxin100, OU=chiyanying, CN=liu
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-11-02 01:18:36+00:00
Valid To: 2029-06-02 01:18:36+00:00
Issuer: C=china, ST=henan, L=luoyang, O=tianxin100, OU=chiyanying, CN=liu
Serial Number: 0x6f56d42e
Hash Algorithm: sha256
md5: 7ef4e45da6a109a7ad435f8991ab7de9
sha1: 7c37a9755f6906e6ab769771edae9cce036d7b03
sha256: aac3df71636333717abfbac5a205dc2621681063a312f69a8e22ab662689c31a
sha512: e50188ab4e0dbc2b2babea67e4efcf58967faa25cd80b78cf8e0db3ba2b2cfbdba603137627b9822234fb6370dcada75fbf8bc554605563428454429dc933346
PublicKey Algorithm: rsa

Bit Size: 1024
Fingerprint: b9a77289e0b02ef9e383bcd9a4c3fcb592e7048d76e6d5fe586617989742b82d

## 应用内通信

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| io.dcloud.appstream.StreamAppMainActivity | Schemes: streamapp://, streamappmain://, |

## 加壳分析

| 文件列表 | 分析结果 |
| --- | --- |
| classes.dex | 壳列表 / 详细情况<br>反虚拟机: Build.FINGERPRINT check<br>Build.MODEL check<br>Build.MANUFACTURER check<br>Build.PRODUCT check<br>SIM operator check<br>device ID check<br>subscriber ID check<br>possible VM check<br>编译器: r8 without marker (suspicious) |