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

**奈斯漫画（ 1.10.5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 | 奈斯漫画 |
| 版本 | 1.10.5 |
| 包名 | cn.djsan2ym.jjdsbawh.ds |
| 域名线索 | 30条 |
| URL线索 | 45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 | nice\_58.apk |
| 文件大小 | 17.23MB |
| MD5值 | 3a5f2a158d23aec155e46cedfbb6bba4 |
| SHA1值 | 021431d89668e38312c3aa0af987e64c131ce1d8 |
| SHA256值 | b8446e06cd308e0dbc25ebe18559ff039e3e8e8dda974c558c30c014396e63a1 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | 奈斯漫画 |
| 包名 | cn.djsan2ym.jjdsbawh.ds |
| 主活动Activity | com.nice.comic.watch.ui.launch.activity.LaunchActivity |
| 安卓版本名称 | 1.10.5 |
| 安卓版本 | 1105 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| long.open.weixin.qq.com | IP: 109.244.217.35 所属国家: China 地区: Beijing 城市: Beijing  |
| xmlpull.org | IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California  |
| mpush-api.aliyun.com | IP: 106.11.172.6 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| docs.realm.io | IP: 104.18.7.238 所属国家: United States of America 地区: California 城市: San Francisco  |
| aaid.umeng.com | IP: 218.91.197.67 所属国家: China 地区: Jiangsu 城市: Nantong  |
| mhapi.spdchgj.com | IP: 8.210.65.242 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| realm.mongodb.com | IP: 18.138.56.176 所属国家: Singapore 地区: Singapore 城市: Singapore  |
| www.openssl.org | IP: 104.65.167.66 所属国家: United States of America 地区: Washington 城市: Seattle  |
| alogus.umeng.com | IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing  |
| ouplog.umeng.com | IP: 47.246.110.94 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| plbslog.umeng.com | IP: 36.156.202.73 所属国家: China 地区: Beijing 城市: Beijing  |
| issuetracker.google.com | IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View  |
| developer.umeng.com | IP: 59.82.31.210 所属国家: China 地区: Beijing 城市: Beijing  |
| xml.apache.org | IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco  |
| github.com | IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond  |
| open.weixin.qq.com | IP: 175.24.219.72 所属国家: China 地区: Beijing 城市: Beijing  |
| jacknc.oss-cn-shanghai.aliyuncs.com | IP: 106.14.229.53 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| alogsus.umeng.com | IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing  |
| ulogs.umengcloud.com | IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing  |
| c-adash.m.taobao.com | IP: 59.82.39.12 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| realm.io | IP: 13.224.141.97 所属国家: Japan 地区: Tokyo 城市: Tokyo  |
| pslog.umeng.com | IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| errlog.umeng.com | IP: 223.109.148.180 所属国家: China 地区: Beijing 城市: Beijing  |
| errlogos.umeng.com | IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| www.google.com | IP: 108.160.165.48 所属国家: United States of America 地区: California 城市: San Francisco  |
| vapi.ucfma.com | IP: 47.242.40.241 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| api.ucfma.com | IP: 47.57.189.83 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong  |
| schemas.android.com | 没有服务器地理信息.  |
| adash.m.taobao.com | IP: 59.82.39.13 所属国家: China 地区: Zhejiang 城市: Hangzhou  |
| ulogs.umeng.com | IP: 223.109.148.141 所属国家: China 地区: Beijing 城市: Beijing  |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0  | io/reactivex/rxjava3/exceptions/UndeliverableException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling  | io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Observable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Single.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Completable.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Maybe.java  |
| https://github.com/ReactiveX/RxJava/wiki/Plugins  | io/reactivex/rxjava3/core/Flowable.java  |
| https://realm.io/news/android-installation-change/  | io/realm/RealmConfiguration.java  |
| https://realm.io/docs/java/latest/  | io/realm/RealmConfiguration.java  |
| https://github.com/Kotlin/kotlinx.coroutines  | io/realm/RealmConfiguration.java  |
| https://issuetracker.google.com/issues/36918154  | io/realm/Realm.java  |
| https://realm.io/docs/java/latest/  | io/realm/RealmObject.java  |
| https://realm.mongodb.com  | io/realm/mongodb/AppConfiguration.java  |
| https://docs.realm.io/sync/using-synced-realms/errors  | io/realm/mongodb/sync/SyncSession.java  |
| https://jacknc.oss-cn-shanghai.aliyuncs.com/api.json.txt  | com/nice/comic/watch/BuildConfig.java  |
| http://api.ucfma.com  | com/nice/comic/watch/BuildConfig.java  |
| http://vapi.ucfma.com  | com/nice/comic/watch/BuildConfig.java  |
| https://jacknc.oss-cn-shanghai.aliyuncs.com/api.json.txt  | com/nice/comic/watch/ui/launch/vm/LaunchVModel$getApiDomain$1.java  |
| https://jacknc.oss-cn-shanghai.aliyuncs.com/api.json.txt  | com/nice/comic/watch/net/ApiConstants.java  |
| http://mhapi.spdchgj.com  | com/nice/comic/watch/net/retrofit/RetrofitClient.java  |
| https://www.google.com  | com/nice/comic/watch/net/retrofit/BaseParamsInterceptorKT.java  |
| https://www.google.com  | com/nice/comic/watch/net/retrofit/HeaderInterceptorKT.java  |
| https://www.google.com  | com/nice/comic/watch/net/imageloader/glide/ImgDecodeInterceptor.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SlidingTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/CommonTabLayout.java  |
| http://schemas.android.com/apk/res/android  | com/flyco/tablayout/SegmentTabLayout.java  |
| https://errlogos.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/upload  | com/uc/crashsdk/e.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/uc/crashsdk/a/h.java  |
| https://errlog.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com  | com/uc/crashsdk/a/d.java  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/controller/ControllerCenter.java  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | com/efs/sdk/base/core/f/c.java  |
| http://xml.apache.org/xslt  | com/elvishew/xlog/formatter/message/xml/DefaultXmlFormatter.java  |
| https://mpush-api.aliyun.com/v2.0/a/audid/req/  | com/ta/a/d/h.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/b/a/e.java  |
| http://xmlpull.org/v1/doc/features.html  | com/ta/utdid2/b/a/a.java  |
| http://adash.m.taobao.com/rest/abtest  | com/alibaba/sdk/android/tbrest/rest/RestConstants.java  |
| http://c-adash.m.taobao.com/rest/gc  | com/alibaba/sdk/android/tbrest/rest/RestConstants.java  |
| http://adash.m.taobao.com/rest/sur  | com/alibaba/sdk/android/tbrest/rest/RestConstants.java  |
| https://aaid.umeng.com/api/updateZdata  | com/umeng/umzid/ZIDManager.java  |
| https://aaid.umeng.com/api/postZdata  | com/umeng/umzid/ZIDManager.java  |
| https://plbslog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ouplog.umeng.com  | com/umeng/commonsdk/stateless/a.java  |
| https://ulogs.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://alogsus.umeng.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://ulogs.umengcloud.com  | com/umeng/commonsdk/statistics/UMServerURL.java  |
| https://pslog.umeng.com  | com/umeng/commonsdk/vchannel/a.java  |
| https://pslog.umeng.com/  | com/umeng/commonsdk/vchannel/a.java  |
| https://developer.umeng.com/docs/66632/detail/  | com/umeng/commonsdk/debug/UMLogUtils.java  |
| http://developer.umeng.com/docs/66650/cate/66650  | com/umeng/analytics/pro/j.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  |
| https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s  | com/tencent/mm/opensdk/diffdev/a/f.java  |
| https://github.com/vinc3m1  | Mogua Engine V1  |
| https://github.com/vinc3m1/RoundedImageView  | Mogua Engine V1  |
| https://github.com/vinc3m1/RoundedImageView.git  | Mogua Engine V1  |
| https://realm.mongodb.com  | lib/armeabi-v7a/librealm-jni.so  |
| https://errlog.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com/api/crashsdk/logcollect  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlog.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| https://errlogos.umeng.com  | lib/armeabi-v7a/libcrashsdk.so  |
| http://www.openssl.org/support/faq.html  | lib/armeabi-v7a/libijkffmpeg.so  |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| help@realm.io  | lib/armeabi-v7a/librealm-jni.so  |
| ffmpeg-devel@ffmpeg.org  | lib/armeabi-v7a/libijkplayer.so  |

### **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: False 找到 1 个唯一证书 主题: C=86, ST=Badi, L=China, O=IT, OU=RxoCompany, CN=ChenHo 签名算法: rsassa\_pkcs1v15 有效期自: 2021-12-02 08:25:56+00:00 有效期至: 2046-11-26 08:25:56+00:00 发行人: C=86, ST=Badi, L=China, O=IT, OU=RxoCompany, CN=ChenHo 序列号: 0x4a94eb9d 哈希算法: sha256 md5值: 1f74010a3102547b17029cdfb71175b3 sha1值: 498f2be80a78f3730813797c05e0a2dee1a55141 sha256值: 717b652733541ed02be7b7d321685188038e711ed184afa183983cbf07f72e7f sha512值: ea079eba10a541aeb52a1a7957e86f0d4ebe7374dbc742b654704dcb619015c7de9ed564825697e3e662739c65b983e606269b6c7574d4228ac7d4c881ac1bdc 公钥算法: rsa 密钥长度: 2048 指纹: 8990518025d3984bb476d64b7b18f7d418026ca552e669d6b5d18d141435b683**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "key\_word" : "关键字"  |
| "library\_roundedimageview\_author" : "Vince Mi"  |
| "library\_roundedimageview\_authorWebsite" : "https://github.com/vinc3m1"  |
| "modify\_password" : "修改密码"  |
| "password" : "密码"  |
| "user" : "用户"  |

## **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.RECEIVE\_USER\_PRESENT | 未知 | Unknown permission | Unknown permission from android reference |
| 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.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.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.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.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.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.ACCESS\_LOCATION\_EXTRA\_COMMANDS | 正常 | 访问额外的位置提供程序命令 | 访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作 |
| 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.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.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 |
| 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.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.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\_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.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。 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.nice.comic.watch.ui.launch.activity.LaunchActivity | **Schemes**: comic://, **Hosts:** comic.twcr.com,  |

**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。**