



MoGua

奈斯漫画 1.10.5.APK 分析报告



APP名称:

奈斯漫画

包名: cn.djsan2ym.jjdsbawh.ds

域名线索: 30条

URL线索: 45条

邮箱线索: 2条

分析日期: 2025年7月9日

分析平台: [摸瓜APK反编译平台](#)

文件名: nice_58.apk
文件大小: 17.23MB
MD5值: 3a5f2a158d23aec155e46cedfbb6bba4
SHA1值: 021431d89668e38312c3aa0af987e64c131ce1d8
SHA256值: b8446e06cd308e0dbc25ebe18559ff039e3e8e8dda974c558c30c014396e63a1

i APP 信息

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

🔍 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 纬度: 39.907501 经度: 116.397232
xmlpull.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065632 经度: -79.891708
mpush-api.aliyun.com	IP: 106.11.172.6 所属国家: China 地区: Zhejiang

	城市: Hangzhou 纬度: 30.293650 经度: 120.161423
docs.realm.io	IP: 104.18.7.238 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
aaid.umeng.com	IP: 218.91.197.67 所属国家: China 地区: Jiangsu 城市: Nantong 纬度: 32.030281 经度: 120.874718
mhapi.spdchgj.com	IP: 8.210.65.242 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
realm.mongodb.com	IP: 18.138.56.176 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067
www.openssl.org	IP: 104.65.167.66 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.606209 经度: -122.332069

alogus.umeng.com	IP: 223.109.148.178 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ouplog.umeng.com	IP: 47.246.110.94 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
plbslog.umeng.com	IP: 36.156.202.73 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
issuetracker.google.com	IP: 142.251.43.14 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
developer.umeng.com	IP: 59.82.31.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
xml.apache.org	IP: 151.101.2.132 所属国家: United States of America 地区: California 城市: San Francisco

	纬度: 37.775700 经度: -122.395203
github.com	IP: 20.205.243.166 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
open.weixin.qq.com	IP: 175.24.219.72 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
jacknc.oss-cn-shanghai.aliyuncs.com	IP: 106.14.229.53 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
alogsus.umeng.com	IP: 223.109.148.176 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
ulogs.umengcloud.com	IP: 223.109.148.179 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
	IP: 59.82.39.12

c-adash.m.taobao.com	所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
realm.io	IP: 13.224.141.97 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696
pslog.umeng.com	IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423
errlog.umeng.com	IP: 223.109.148.180 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232
errlogos.umeng.com	IP: 47.246.110.18 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.google.com	IP: 108.160.165.48 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700

	经度: -122.395203
vapi.ucfma.com	IP: 47.242.40.241 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
api.ucfma.com	IP: 47.57.189.83 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
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 纬度: 30.293650 经度: 120.161423
ulogs.umeng.com	IP: 223.109.148.141 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232

 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/LaunchVMModel\$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×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/d.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuiid=%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/libijkffmpegpeg.so

 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
-------------------------	---------------------------------

手机线索

手机号	所在文件
17179869184	tv/danmaku/ijk/media/player/IjkMediaMeta.java

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

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"

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.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。

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,