MoGua

蜜獾 1.0.2.APK 分析报告

APP名称: 蜜獾

包名:	com.uuvsnz.wsbogyip
域名线索:	16条
URL线索:	18条
邮箱线索:	5条
分析日期:	2024年9月18日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Mihuan.3.apk
文件大小: 24.28MB

MD5值: ed079e2137df463686f2b45fb45636e6
SHA1值: f2a4e762248667073b0116e3ddd543f6af005165
SHA256值: 1708c9401dd05d1e461392f07987791197ceacb50132bc068cde5fb63fb7d5d8

APP 信息

App名称: 蜜獾
包名: com.uuvsnz.wsbogyip
主活动Activity: com.posta.mihuan.LaunchPageActivity
安卓版本名称: 1.0.2
安卓版本: 8

域名线索

域名	服务器信息
doctor.sadfate.com	没有服务器地理信息.
schemas.android.com	没有服务器地理信息.
mihuan9.com	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.openssl.org	**IP**: 34.49.79.89 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
	IP: 20.205.243.166

github.com	**所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
baidu.com	IP: 110.242.68.66 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
miguan-1323228439.cos.ap-nanjing.myqcloud.com	IP: 112.80.252.187 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
mclient.alipay.com	IP: 125.39.135.57 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.facebook.com	IP: 118.193.240.41 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
plus.google.com	IP: 162.125.7.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

ttt.xyz	**IP**: 13.248.169.48 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
i0.hdslb.com	**IP**: 120.52.51.103 **所属国家**: China **地区**: Hebei **城市**: Langfang **纬度**: 39.509720 **经度**: 116.694717
qijiekou.xyz	**IP**: 16.162.214.131 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
cdn.livechatinc.com	**IP**: 23.200.11.96 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
s3.ap-east-1.amazonaws.com	**IP**: 52.95.162.46 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
qisejiekou.xyz	**IP**: 16.162.214.131 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521

	经度: 114.157692

URL线索

URL信息	Url所在文件
https://github.com/danikula/AndroidVideoCache/issues/88.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues/43.	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula	com/danikula/videocache/HttpUrlSource.java
https://github.com/danikula/AndroidVideoCache/issues.	com/danikula/videocache/HttpUrlSource.java
http://%s:%d/%s	com/danikula/videocache/Pinger.java
https://github.com/danikula/AndroidVideoCache/issues/134.	com/danikula/videocache/Pinger.java
http://%s:%d/%s	com/danikula/videocache/HttpProxyCacheServer.java
https://cdn.livechatinc.com/app/mobile/urls.json	com/livechatinc/inappchat/LoadWebViewContentTask.java
https://.+facebook.+(/dialog/oauth\\?	com/livechatinc/inappchat/ChatWindowView.java
https://www.facebook.com/dialog/return/arbiter	com/livechatinc/inappchat/ChatWindowView.java
http://schemas.android.com/apk/res/android	com/flyco/tablayout/SegmentTabLayout.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
https://miguan-1323228439.cos.ap-nanjing.myqcloud.com/mi.json	com/posta/mihuan/LaunchPageActivity.java

https://s3.ap-east-1.amazonaws.com/ad.lmnykj.com/mi.json	com/posta/mihuan/LaunchPageActivity.java
https://mihuan9.com	com/posta/mihuan/LaunchPageActivity.java
https://baidu.com	com/posta/mihuan/bean/VideoDetailInfoBean.java
https://mclient.alipay.com/h5Continue.htm?	com/posta/mihuan/web/AlipayH5Activity.java
https://i0.hdslb.com/bfs/archive/9312d0c09adec8023e8677eed438742620f0d430.jpg@206w_116h_1c_100q.webp	com/posta/mihuan/home/RecommendListAdapter.java
http://doctor.sadfate.com/uploads/images/20200323/a1a3a534ac62ab56fe9231350f9c814d.gif	com/posta/mihuan/home/RecommendListAdapter.java
http://schemas.android.com/apk/res/android	j/h/a/b/c/y/g.java
https://plus.google.com/	j/h/a/b/d/k/d1.java
https://mihuan9.com	j/n/a/m0.java
https://ttt.xyz/	j/n/a/f2/j.java
https://ttt.xyz/api/user/user_info	j/n/a/f2/j.java
https://ttt.xyz/api/index/index	j/n/a/f2/j.java
https://ttt.xyz/api/live/pingtai	j/n/a/f2/j.java
https://ttt.xyz/api/live/ad_info	j/n/a/f2/j.java
https://ttt.xyz/api/live/zj_list	j/n/a/f2/j.java
https://ttt.xyz/api/video/rank	j/n/a/f2/j.java
https://ttt.xyz/api/home/my_ad	j/n/a/f2/j.java
https://ttt.xyz/api/home/new_zuanti	j/n/a/f2/j.java

https://ip_host.com/api/login/get_ip	j/n/a/f2/j.java
https://ttt.xyz/api/index/loufeng	j/n/a/f2/j.java
https://ttt.xyz/api/pay/gold_meal	j/n/a/f2/j.java
https://ttt.xyz/api/theme	j/n/a/f2/j.java
https://ttt.xyz/api/user/close_history	j/n/a/f2/j.java
https://ttt.xyz/api/home/new_ad	j/n/a/f2/j.java
https://ttt.xyz/api/live	j/n/a/f2/j.java
https://ttt.xyz/api/new_login	j/n/a/f2/j.java
https://ttt.xyz/api/index/app_config	j/n/a/f2/j.java
https://ttt.xyz/api/service	j/n/a/f2/j.java
https://ttt.xyz/api/home/cate	j/n/a/f2/j.java
https://ttt.xyz/api/news	j/n/a/f2/j.java
https://ttt.xyz/api/ranking	j/n/a/f2/j.java
https://ttt.xyz/api/home/guocan	j/n/a/f2/j.java
https://ttt.xyz/api/home/rihan	j/n/a/f2/j.java
https://ttt.xyz/api/home/oumei	j/n/a/f2/j.java
https://ttt.xyz/api/home/dongman	j/n/a/f2/j.java

https://ttt.xyz/api/video/view_list	j/n/a/f2/j.java
https://ttt.xyz/api/video/hot_list	j/n/a/f2/j.java
https://ttt.xyz/api/video/news_list	j/n/a/f2/j.java
https://ttt.xyz/api/video/collect_list	j/n/a/f2/j.java
https://ttt.xyz/api/live/cate	j/n/a/f2/j.java
https://ttt.xyz/api/live/info	j/n/a/f2/j.java
https://ttt.xyz/api/h5/live_list	j/n/a/f2/j.java
https://ttt.xyz/api/H5/ad_live_list	j/n/a/f2/j.java
https://ttt.xyz/api/live/index	j/n/a/f2/j.java
https://ttt.xyz/api/login/ceshi	j/n/a/f2/j.java
https://ttt.xyz/api/home/zuanti	j/n/a/f2/j.java
https://ttt.xyz/api/login/add_agent	j/n/a/f2/j.java
https://ttt.xyz/api/ent/loufeng	j/n/a/f2/j.java
https://ttt.xyz/api/login/shixiao	j/n/a/f2/j.java
https://ttt.xyz/api/search_list	j/n/a/f2/j.java
https://ttt.xyz/api/video/video_info	j/n/a/f2/j.java
https://ttt.xyz/api/user/collect_list	j/n/a/f2/j.java
https://ttt.xyz/api/user/add_history	j/n/a/f2/j.java

https://ttt.xyz/api/notice	j/n/a/f2/j.java
https://ttt.xyz/api/version	j/n/a/f2/j.java
https://ttt.xyz/api/ad_up	j/n/a/f2/j.java
https://ttt.xyz/	j/n/a/f2/b.java
https://qisejiekou.xyz/	j/n/a/f2/b.java
https://ip_host.com/	j/n/a/f2/b.java
https://qijiekou.xyz/	j/n/a/f2/b.java
http://www.openssl.org/support/faq.html	lib/armeabi-v7a/libijkffmpeg.so

邮箱线索

邮箱地址	所在文件
qisemao8@gmail.com	com/posta/mihuan/widget/CusCenterDialog.java
d438742620f0d430.jpg@206w_116h_1c_100q.webp	com/posta/mihuan/home/RecommendListAdapter.java
qisemao8@gmail.com	com/posta/mihuan/fragment/MeFragment.java
u0013android@android.com0 u0013android@android.com	j/h/a/b/d/u.java
ffmpeg-devel@ffmpeg.org	lib/armeabi-v7a/libijkplayer.so

手机线索

手机号	所在文件
17512775099	j/h/b/d/a.java
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: True
找到 1 个唯一证书
主题: C=Bs, ST=eecaiP, L=Ahphe, O=xUK, OU=xUK, CN=xUK
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-01 07:00:22+00:00
有效期至: 2124-07-08 07:00:22+00:00
发行人: C=Bs, ST=eecaiP, L=Ahphe, O=xUK, OU=xUK, CN=xUK
序列号: 0x4f29a40b
哈希算法: sha512
md5值: e1f20db69b8f9d4c9016959b72fbe0cc
sha1值: fed9d93a3c45c3579b72a6cb3b1fa31289477a00
sha256值: 0de411f843f74e280d1c9917151f542348688229925cce25a43d2389533fc3a9
sha512值: c0883500893c042f245974e63ed3db2019bd934bd478c752f016ea174f35b50786c6c6e30a50206210075fea159db305ec057ba98b3dcfb649884efb8af53ed2
公钥算法: rsa
密钥长度: 2048
指纹: fe157c68e8791ec12c86933cd85069c7f192a4eaea2c51653388a3b0c0dca952

硬编码敏感信息

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.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.MANAGE_EXTERNAL_STORAGE	危险	允许应用程序广泛访问范围存储中的外部存储	允许应用程序广泛访问范围存储中的外部存储。旨在供少数需要代表用户管理文件的应用程序使用
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.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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。

应用内通信