



MoGua

N号房 1.1.1.APK 分析报告



APP名称:

N号房

包名:	com.zq.nhf
域名线索:	35条
URL线索:	16条
邮箱线索:	3条
分析日期:	2025年8月14日
分析平台:	摸瓜APK反编译平台

文件名: nhfss002_2024.8.20.400.apk
文件大小: 11.87MB
MD5值: 9ab8c5d8c1d0e4c1cbfdb0761bd465a2
SHA1值: 171291da3a41b81df224967bd7d4da47b99b9e6b
SHA256值: 9ea80b497ceeeb53d734f4402372677f71a11b26b145ca452019e978982f1eed

i APP 信息

App名称: N号房
包名: com.zq.nhf
主活动Activity: com.zq.douyin.MainActivity
安卓版本名称: 1.1.1
安卓版本: 3

🔍 域名线索

域名	服务器信息
lf3-cdn-tos.bdxiguastatic.com	IP: 42.59.6.90 所属国家: China 地区: Liaoning 城市: Dalian 纬度: 41.069592 经度: 122.598511
cdn.plyr.io	IP: 104.27.195.88 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
html2canvas.hertzen.com	IP: 172.67.140.170 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
go.aniview.com	IP: 104.120.120.147 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
pan.baidu.com	IP: 110.242.69.176 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
brianleroux.github.com	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
t.me	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
aomedia.org	IP: 185.199.110.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
	IP: 104.16.227.18

jsperf.com	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
swiperjs.com	没有服务器地理信息.
d3n2vdp1h9ohbb.cloudfront.net	IP: 13.33.100.176 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
rm.zkbsw.cc	IP: 103.190.125.14 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
ldy.nroom10.com	IP: 106.74.25.198 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
imasdk.googleapis.com	IP: 114.250.65.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
issues.apache.org	IP: 168.119.33.54 所属国家: Germany 地区: Bayern 城市: Gunzenhausen

	纬度: 48.323860 经度: 11.601019
hertzen.com	IP: 104.21.65.51 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
cres.rqi564.com	IP: 103.39.108.219 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
cdn.jsdelivr.net	IP: 8.7.198.46 所属国家: United States of America 地区: Louisiana 城市: Monroe 纬度: 32.548328 经度: -92.045235
i.ytimg.com	IP: 168.143.162.58 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
noembed.com	IP: 151.101.129.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 20.205.243.166 所属国家: Singapore

github.com	地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
player.vimeo.com	IP: 157.240.17.35 所属国家: Switzerland 地区: Zurich 城市: Zurich 纬度: 47.366825 经度: 8.549790
www.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
www.youtube-nocookie.com	IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
bk.dlkxi.cc	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
www.youtube.com	IP: 199.16.158.182 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446

raw.githubusercontent.com	IP: 185.199.109.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
www.w3.org	IP: 104.18.23.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
hfive.qsxon.com	IP: 104.21.40.242 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
axios-http.com	IP: 18.139.194.139 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
img01.yzcdn.cn	IP: 221.15.70.53 所属国家: China 地区: Henan 城市: Luoyang 纬度: 34.683289 经度: 112.453911
developer.mozilla.org	IP: 34.111.97.67 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731

	经度: -94.578568
43.231.0.225	IP: 43.231.0.225 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
34.150.33.40	IP: 34.150.33.40 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
vimeo.com	IP: 31.13.88.26 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249

 URL线索

URL信息	Url所在文件
https://cdn.jsdelivr.net/npm/workbox-cdn@5.1.4/workbox	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://jsperf.com/b64tests	摸瓜V2引擎
http://server/myapp/index.html	摸瓜V2引擎

https://issues.apache.org/jira/browse/CB-11522)	摸瓜V2引擎
https://html2canvas.hertzen.com >	摸瓜V2引擎
https://hertzen.com >	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://developer.mozilla.org/fr/docs/Web/API/CustomEvent	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
http://brianleroux.github.com/lawnchair/),	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://cdn.plyr.io/3.7.2/plyr.svg	摸瓜V2引擎
https://cdn.plyr.io/static/blank.mp4	摸瓜V2引擎
https://player.vimeo.com/api/player.js	摸瓜V2引擎

https://player.vimeo.com/video/	摸瓜V2引擎
https://vimeo.com/api/oembed.json?url=	摸瓜V2引擎
https://www.youtube.com/iframe_api	摸瓜V2引擎
https://noembed.com/embed?url=https://www.youtube.com/watch?v=	摸瓜V2引擎
https://imasdk.googleapis.com/js/sdkloader/ima3.js	摸瓜V2引擎
https://www.youtube-nocookie.com	摸瓜V2引擎
http://www.youtube.com	摸瓜V2引擎
https://i.ytimg.com/vi/	摸瓜V2引擎
https://go.aniview.com/api/adserver6/vast/	摸瓜V2引擎
https://hfive.qsxon.com	摸瓜V2引擎
https://t.me/	摸瓜V2引擎
https://lf3-cdn-tos.bdxiguastatic.com/obj/ixigua-static/xigua_fe/xigua_video_web_pc/static/media/series.bd5583e1.gif	摸瓜V2引擎
https://pan.baidu.com/s/1wPIQE5srd_cGuPVqBWNUxw?pwd=1234	摸瓜V2引擎
https://ldy.nroom10.com:19999/nhft001	摸瓜V2引擎
https://cres.rqi564.com	摸瓜V2引擎
https://43.231.0.225:19888/api/v1	摸瓜V2引擎
https://34.150.33.40:19888/api/v1	摸瓜V2引擎
https://hk.dlxi.cc/api/v1	摸瓜V2引擎

https://rm.zkbsw.cc/api/v1	摸瓜V2引擎
https://d3n2vdp1h9ohbb.cloudfront.net/api/v1	摸瓜V2引擎
https://aomedia.org/emsg/ID3	摸瓜V2引擎
https://github.com/mathiasbynens/CSS.escape).	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.37.1/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	摸瓜V2引擎
http://x	摸瓜V2引擎
https://github.com/crypto-browserify/crypto-browserify	摸瓜V2引擎
https://img01.yzcdn.cn/vant/share-sheet-	摸瓜V2引擎
https://img01.yzcdn.cn/vant/empty-image-	摸瓜V2引擎
http://swiperjs.com\n	摸瓜V2引擎
https://github.com/indutny/elliptic/issues	摸瓜V2引擎
https://github.com/indutny/elliptic	摸瓜V2引擎
https://github.com/axios/axios.git	摸瓜V2引擎

https://github.com/axios/axios/issues	摸瓜V2引擎
https://axios-http.com	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
solderzzc@gmail.com stefano.magrassi@gmail.com	摸瓜V2引擎
sy12god@gmail.com	摸瓜V2引擎
git@github.com fedor@indutny.com	摸瓜V2引擎

 手机线索

手机号	所在文件
13411538969	defpackage/l7.java
14622674786	defpackage/xd.java
15351175428	defpackage/wb.java
17890589254	defpackage/qu.java
17210090653	defpackage/s5.java

19847420677	defpackage/sn.java
17145714854	defpackage/ya.java
15702333322	defpackage/ma.java
19919152923	摸瓜V2引擎

🌟 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=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-20 00:14:52+00:00
有效期至: 2052-01-06 00:14:52+00:00
发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
序列号: 0x41ae68df
哈希算法: sha256
md5值: 21fdc1d901bce0a742d75d1a7a0faaeb
sha1值: cf55947c7d8fa1dd0ad9be14b0dae3b80d1e67d6
sha256值: bebbbc4959edf561e2b2520387736cdcc87336007e0947387e5d3d6a33ca0c6e6
sha512值: 5658040192badd86001f462a0044802a7599d482b4dfd51d1efaf9baaac5647d6234ac517d1b8691d220d92dd09356f8d222aa91c89112c3ddeba07b819f4d9c
公钥算法: rsa
密钥长度: 2048
指纹: 3d156e714e80c135833b4f865de43624cd4e0a197cf85e1e5aa726999b9c5ac2

🔑 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.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.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.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

应用内通信

报告由 [摸瓜APK反编译平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。