



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:	36条
URL线索:	16条
邮箱线索:	3条
分析日期:	2025年9月14日
分析平台:	摸瓜APK反编译平台

文件名: N号房.apk
文件大小: 12.21MB
MD5值: 5b171b23c0e8cfdb7cb5d8c6f55629ea
SHA1值: 2cd3c659d56dcedcc1ecf061aa9f19a8a9dd62b0
SHA256值: 102b30c53161845e574109c79032665619e4b72fbbbc3f38ed26f0b6e588d99

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
brianleroux.github.com	IP: 185.199.111.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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
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
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
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
imasdk.googleapis.com	IP: 114.250.67.33 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
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
go.aniview.com	IP: 23.205.198.54 所属国家: United States of America 地区: California 城市: El Segundo 纬度: 33.919201 经度: -118.416580
	IP: 172.67.140.170

html2canvas.hertzen.com	所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
d3n2vdp1h9ohbb.cloudfront.net	IP: 3.165.16.174 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
pan.baidu.com	IP: 110.242.69.174 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
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
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
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

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
aomedia.org	IP: 185.199.108.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
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
jsperf.com	IP: 104.16.228.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
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
i.ytimg.com	IP: 162.125.34.133 所属国家: United States of America 地区: California

	城市: San Francisco 纬度: 37.775700 经度: -122.395203
bk.dlkxi.cc	IP: 46.149.202.180 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
lf3-cdn-tos.bdxiguastatic.com	IP: 119.167.184.217 所属国家: China 地区: Shandong 城市: Qingdao 纬度: 36.098610 经度: 120.371941
www.youtube.com	IP: 31.13.68.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
kk.xcdwt.com	IP: 103.190.125.20 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: 151.101.89.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203

t.me	IP: 149.154.167.99 所属国家: United Kingdom of Great Britain and Northern Ireland 地区: England 城市: Warrington 纬度: 52.184460 经度: -0.687590
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
swiperjs.comn	没有服务器地理信息.
cdn.plyr.io	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
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
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
	IP: 31.13.94.36 所属国家: Argentina

player.vimeo.com	地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
101.132.69.237	IP: 101.132.69.237 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
cres.rqi564.com	IP: 43.252.173.22 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
www.youtube-nocookie.com	IP: 142.251.211.238 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
github.com	IP: 20.205.243.166 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281

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
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/stefannener/es6-promise/master/LICENSE	摸瓜V2引擎

https://raw.githubusercontent.com/standard-schema/standard-schema/master/LICENSE	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://kk.xcdwt.com/api/v1/	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://bk.dlkxi.cc/api/v1/	摸瓜V2引擎
https://d3n2vdp1h9ohbb.cloudfront.net/api/v1/	摸瓜V2引擎
https://101.132.69.237:16888/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	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
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.vtime.com/vi/	摸瓜V2引擎

https://nyang.com/vr	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

 邮箱线索

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

 手机线索

--	--

手机号	所在文件
14561889529	defpackage/h1.java
16831672527	defpackage/re.java
13408987892	defpackage/ui.java
18156170580	defpackage/a8.java
18156170580	defpackage/b0.java
19067067199	defpackage/b0.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: 2024-09-13 06:27:08+00:00

有效期至: 2052-01-30 06:27:08+00:00

发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com

序列号: 0x2191ad59

哈希算法: sha256

md5值: 2b7ff09df16ec978d8d6c3f193eae4bd

sha1值: 9539522a1245756596a77c8fcdf3b41d9166b4e4

sha256值: fbda59a02e6031dad638a593e338685fd6c947cc6daba55cea6ee2662222c7e6

sha512值: 02a3f720196a25af4c823bd85d6d4d1cc74ada09baff3cd1ba72fc7b314fe427cfeb72441bf63da1f1c97888d4891407f4de4a1ca9fd37634f6a2fbf0debde67

公钥算法: rsa

密钥长度: 2048

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。