MoGua

Kikoeru 2.11.0.APK 分析报告

APP名称:	Kikoeru

包名:	com.cnl.kikoeru
域名线索:	42条
URL线索:	34条
邮箱线索:	0条
分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Kikoeru_2.11.0.apk
文件大小: 5.84MB
MD5值: b8ffa157aac4f52ef50a0c80d1c4b903
SHA1值: cdbf41039556a0e502c20c84a4af882d3efe6f1b
SHA256值: d4e35e35a7020dd427ab494a55a44f15a4f6a8d1fc706d004c10cfcaa09e6f97

APP 信息

App名称: Kikoeru
包名: com.cnl.kikoeru
主活动Activity: com.cnl.kikoeru.MainActivity
安卓版本名称: 2.11.0
安卓版本: 57

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
goo.gle	**IP**: 67.199.248.13 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.750134 **经度**: -73.997009
part-0012.t-0009.t-msedge.net	**IP**: 13.107.246.40 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903

schemas.microsoft.com	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
developer.apple.com	**IP**: 17.253.87.198 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
dns.alidns.com	**IP**: 223.5.5.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
api-free.deepl.com	**IP**: 172.65.225.25 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www2.deepl.com	**IP**: 172.65.212.243 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
part-0032.t-0009.t-msedge.net	**IP**: 13.107.246.60 **所属国家**: United States of America **地区**: Washington **城市**: Redmond

	纬度: 47.682899 **经度**: -122.120903
in2-gw2-01-ce7dd027.eastus2.cloudapp.azure.com	没有服务器地理信息.
developer.android.com	IP: 142.251.33.110 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
install.appcenter.ms	IP: 13.107.246.73 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
api.asmr-200.com	IP: 172.67.215.121 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
shed.dual-low.part-0012.t-0009.t-msedge.net	IP: 13.107.246.40 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
dashif.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

mobile.events.data.microsoft.com	**IP**: 20.189.173.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
s-part-0010.t-0009.t-msedge.net	**IP**: 13.107.246.38 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
www.dlsite.com	**IP**: 185.45.7.97 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: London **纬度**: 51.508530 **经度**: -0.125740
api.asmr.one	**IP**: 104.21.50.254 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.gstatic.com	**IP**: 203.208.43.98 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
front-door-ead5eebugwa5ayfd.z01.azurefd.net	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond

	纬度: 47.682899 **经度**: -122.120903
android.googlesource.com	IP: 142.250.99.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
api.asmr-100.com	IP: 172.67.215.121 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
in.appcenter.ms	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
shed.dual-low.part-0032.t-0009.t-msedge.net	IP: 13.107.246.60 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
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
	IP: 127.0.0.1

g.co	**所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
default.url	没有服务器地理信息.
api.appcenter.ms	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
in2-prod-east-us2-23fa330.trafficmanager.net	**IP**: 4.152.45.219 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
translate.google.com	**IP**: 142.250.217.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
aomedia.org	**IP**: 45.114.11.25 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322
in2-gw2-03-3d6c3051.eastus2.cloudapp.azure.com	**IP**: 20.57.103.21 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton

	纬度: 36.667641 **经度**: -78.387497
connectivitycheck.gstatic.com	**IP**: 203.208.39.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
ns.adobe.com	没有服务器地理信息.
star-azurefd-prod.trafficmanager.net	**IP**: 13.107.246.74 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
issuetracker.google.com	**IP**: 142.251.33.78 **所属国家**: Canada **地区**: Ontario **城市**: Toronto **纬度**: 43.653660 **经度**: -79.382927
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
www.asmr-300.com	**IP**: 172.67.215.121 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

zone-split.asmr-300.com	没有服务器地理信息.
translate.googleapis.com	**IP**: 142.251.215.234 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
api.asmr-300.com	**IP**: 172.67.215.121 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://www.asmr-300.com/playlist?id=	D0/C0113a.java
https://issuetracker.google.com/issues/new?component=413106	J2/Q0.java
http://dashif.org/guidelines/trickmode	G1/d.java
http://dashif.org/guidelines/trickmode	H1/e.java
http://dashif.org/guidelines/last-segment-number	H1/e.java
http://schemas.android.com/apk/res/android	J0/I.java
	J1/E.java

http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense	
https://x</LA_URL>	J1/D.java
https://default.url	J1/D.java
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	A1/A.java
http://g.co/dev/packagevisibility.	A1/G.java
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	D1/N.java
https://goo.gle/compose-feedback	P/AbstractC0798t.java
https://api-free.deepl.com/v2/translate	f4/d.java
https://www2.deepl.com/jsonrpc	f4/u.java
https://install.appcenter.ms	X2/c.java
http://ns.adobe.com/xap/1.0/	g2/C1542a.java
https://www.asmr-300.com/playlist?id=	r/Z.java
https://dns.alidns.com/dns-query	com/cnl/kikoeru/MainApplication.java
https://api.appcenter.ms/v0.1	com/microsoft/appcenter/distribute/Distribute.java
http://ns.adobe.com/xap/1.0/\u0000	n1/C1947g.java
https://translate.googleapis.com/translate_a/t	e4/t.java
https://translate.google.com/	e4/t.java
https://translate.googleapis.com/translate_a/element.js	e4/x.java

https://translate.google.com/	e4/x.java
https://in.appcenter.ms	W4/c.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	W4/c.java
https://aomedia.org/emsg/ID3	j2/C1701a.java
https://developer.apple.com/streaming/emsg-id3	j2/C1701a.java
https://www.asmr-300.com	G3/n.java
https://api.asmr.one	d7/C1360h.java
https://www.dlsite.com/maniax/work/=/product_id/	V3/C0948v.java
https://www.asmr-300.com/work/	V3/C0945s.java
https://issuetracker.google.com/issues/new?component=413106	K2/c.java
https://.+/api/cover/RJ(\\d	u3/e.java
https://api.asmr.one	A3/b.java
https://api.asmr-100.com	A3/b.java
https://api.asmr-200.com	A3/b.java
https://api.asmr-300.com	A3/b.java
https://www.asmr-300.com/work/	A3/b.java
https://api.asmr-300.com	A3/a.java

https://t.me/+hZALL6s4hexhZjY1	L3/e.java
https://dns.alidns.com/dns-query	P3/a.java
https://www.asmr-300.com/playlist?id=	摸瓜V3引擎
part-0012.t-0009.t-msedge.net	摸瓜V3引擎
https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
https://t.me/	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
https://translate.googleapis.com/translate_a/element.js	摸瓜V3引擎
https://translate.googleapis.com/translate_a/t	摸瓜V3引擎
part-0032.t-0009.t-msedge.net	摸瓜V3引擎
in2-gw2-01-ce7dd027.eastus2.cloudapp.azure.com	摸瓜V3引擎
instantmessaging-pa.googleapis.com	摸瓜V3引擎
infinitedata-pa.googleapis.com	摸瓜V3引擎
https://api.asmr-300.com	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
shed.dual-low.part-0012.t-0009.t-msedge.net	摸瓜V3引擎
http://g.co/dev/packagevisibility.	摸瓜V3引擎
https://api.appcenter.ms/v0.1	摸瓜V3引擎

https://api.asmr-100.com	摸瓜V3引擎
s-part-0010.t-0009.t-msedge.net	摸瓜V3引擎
http://dashif.org/guidelines/thumbnail_tile	摸瓜V3引擎
www.gstatic.com	摸瓜V3引擎
www.googleapis.com	摸瓜V3引擎
http://dashif.org/thumbnail_tile	摸瓜V3引擎
https://api.asmr-200.com	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
front-door-ead5eebugwa5ayfd.z01.azurefd.net	摸瓜V3引擎
http://dashif.org/guidelines/trickmode	摸瓜V3引擎
https://aomedia.org/emsg/ID3	摸瓜V3引擎
in.appcenter.ms	摸瓜V3引擎
shed.dual-low.part-0032.t-0009.t-msedge.net	摸瓜V3引擎
api.asmr-300.com	摸瓜V3引擎
https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted	摸瓜V3引擎
https://goo.gle/compose-feedback	摸瓜V3引擎
firebaseinstallations.googleapis.com	摸瓜V3引擎

api.appcenter.ms	摸瓜V3引擎
growth-pa.googleapis.com	摸瓜V3引擎
in2-prod-east-us2-23fa330.trafficmanager.net	摸瓜V3引擎
https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread	摸瓜V3引擎
https://www2.deepl.com/jsonrpc	摸瓜V3引擎
https://www.asmr-300.com/work/	摸瓜V3引擎
https://www.dlsite.com/maniax/work/=/product_id/	摸瓜V3引擎
in2-gw2-03-3d6c3051.eastus2.cloudapp.azure.com	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
star-azurefd-prod.trafficmanager.net	摸瓜V3引擎
https://default.url	摸瓜V3引擎
https://install.appcenter.ms	摸瓜V3引擎
https://api.asmr.one	摸瓜V3引擎
zone-split.asmr-300.com	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
play.googleapis.com	摸瓜V3引擎
http://dashif.org/guidelines/last-segment-number	摸瓜V3引擎
https://dns.alidns.com/dns-query	摸瓜V3引擎

https://in.appcenter.ms	摸瓜V3引擎
https://www.asmr-300.com	摸瓜V3引擎
https://api-free.deepl.com/v2/translate	摸瓜V3引擎

邮箱线索

手机线索

手机号	所在文件
17512775099	r4/AbstractC2363a.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: CN=内个谁
签名算法: rsassa_pkcs1v15
有效期自: 2018-03-05 05:13:41+00:00
有效期至: 2118-02-09 05:13:41+00:00
发行人: CN=内个谁
序列号: 0x1
哈希算法: sha256
md5值: 00ecbc1bbd94fe44b3925233ca5e7770
sha1值: 422971f3148485f19564fb6948904e4168a881fc
sha256值: 6f2c8ed65e470ec8ddcb2165de3bfb173a515ef3fff19e6cc7f79ce84df5742d

sha512值: 4f27a5e468d505b91eef392dbd5933ff34dbb601ba70df3038841128465d320d5aa9d43ce6c43701e3ad25aeefa6ee41b1f63229921ed7f200dab020a8224575
公钥算法: rsa
密钥长度: 1024
指纹: 3cb3f1bc0bf746aa9061f59c596306a5f4db214d83d477ed6befaed8439e043e

🔑 硬编码敏感信息

可能的敏感信息
"password" : "password"
"privacy_private" : "Private"
"token_exp_auto_login_failed" : "Login expired on %1$s, please try to login again"
"username" : "username"
"password" : "パスワード"
"privacy_private" : "プライベート"
"token_exp_auto_login_failed" : "ログインの有効期限が %1$s に切れました。もう一度ログインしてください。"
"username" : "ユーザー名"
"password" : "密碼"
"privacy_private" : "私有"
"token_exp_auto_login_failed" : "登入已於%1$s過期，請嘗試重新登陸"
"username" : "用戶名"
"password" : "密码"

"privacy_private" : "私有"
"token_exp_auto_login_failed" : "登录已于%1$s过期，请尝试重新登陆"
"username" : "用户名"
"password" : "密碼"
"privacy_private" : "私有"
"token_exp_auto_login_failed" : "登入已於%1$s過期，請嘗試重新登陸"
"username" : "用戶名"

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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE_DATA_SYNC	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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
com.cnl.kikoeru.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference
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.DOWNLOAD_WITHOUT_NOTIFICATION	未知	Unknown permission	Unknown permission from android reference

android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.cnl.kikoeru.MainActivity	Schemes: https://, Hosts: asmr.one, *.asmr.one, asmr-100.com, *.asmr-100.com, asmr-200.com, *.asmr-200.com, asmr-300.com, *.asmr-300.com,
com.microsoft.appcenter.distribute.DeepLinkActivity	Schemes: appcenter://, Hosts: updates, Paths: /,

---