



Via 5.1.1.APK 分析报告



APP名称:

Via

包名:	mark.via
域名线索:	55条
URL线索:	47条
邮箱线索:	4条
分析日期:	2025年8月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: via-release-cn.apk

文件大小: 1.73MB

MD5值: 3753d5c91e7ad73e5dc162506fa0b499

SHA1值: c9d90892c3533ad55d6d16be4214c769039126a6
SHA256值: 07e4cd45b5f09fefc4846f30f739a5061f56ce26104b5af7e697a67b9282c629

i APP 信息

App名称: Via
包名: mark.via
主活动Activity: mark.via.Shell
安卓版本名称: 5.1.1
安卓版本: 20231110

🔍 域名线索

域名	服务器信息
m.baidu.com	IP: 110.242.68.9 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
app.viayoo.com	IP: 47.98.219.161 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
viayoo.com	IP: 172.67.186.34 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 112.64.200.23

st.so.com	所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
raw.githubusercontent.com	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
suggestion.baidu.com	IP: 163.177.17.122 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
clients1.google.com	IP: 172.217.160.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
api.bing.com	IP: 13.107.5.80 所属国家: United States of America 地区: Washington 城市: Redmond 纬度: 47.682899 经度: -122.120903
3d.iqdb.org	IP: 91.121.210.31 所属国家: France 地区: Hauts-de-France 城市: Roubaix 纬度: 50.693710 经度: 3.174439
	IP: 203.208.50.98

www.gstatic.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
dav.jianguoyun.com	IP: 118.186.60.194 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
yandex.ru	IP: 77.88.55.88 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
violentmonkey.github.io	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
m.so.com	IP: 42.236.98.98 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
my.cdn.com	没有服务器地理信息.
www.sogou.com	IP: 61.135.158.87 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

coolapk.com	IP: 218.12.71.58 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
data.flurry.com	IP: 69.147.88.7 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
www.so.com	IP: 42.236.9.70 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
help.eyeo.com	IP: 88.99.84.224 所属国家: Germany 地区: Sachsen 城市: Falkenstein 纬度: 50.477852 经度: 12.371563
wap.sogou.com	IP: 61.135.158.193 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tineye.com	IP: 199.96.59.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968

	经度: -122.410446
ascii2d.net	IP: 104.26.5.72 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
yandex.com	IP: 5.255.255.80 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
trace.moe	IP: 172.67.80.163 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
twitter.com	IP: 59.188.250.54 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
iqdb.org	IP: 91.121.210.31 所属国家: France 地区: Hauts-de-France 城市: Roubaix 纬度: 50.693710 经度: 3.174439
file-examples.com	IP: 185.135.88.81 所属国家: Poland 地区: Wielkopolskie 城市: Poznan

	纬度: 52.406914 经度: 16.930000
support.qq.com	IP: 116.130.229.78 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
webtrans.yodao.com	IP: 103.74.50.106 所属国家: China 地区: Guangdong 城市: Guangzhou 纬度: 23.127361 经度: 113.264572
www.google.com	IP: 104.244.46.5 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
weibo.com	IP: 202.108.0.98 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
res.viayoo.com	IP: 104.21.19.117 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
	IP: 42.236.98.67 所属国家: China 地区: Henan

sug.so.360.cn	城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
so.toutiao.com	IP: 122.14.230.133 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
duckduckgo.com	IP: 74.86.226.234 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
fanyi.baidu.com	IP: 110.242.68.186 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
yz.m.sm.cn	IP: 59.82.23.55 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
lens.google.com	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
	IP: 146.75.113.229 所属国家: Sweden

fastly.jsdelivr.net	地区: Vastra Gotalands lan 城市: Goeteborg 纬度: 57.707409 经度: 11.966732
cfg.flurry.com	IP: 98.136.147.20 所属国家: United States of America 地区: New York 城市: New York City 纬度: 40.731323 经度: -73.990089
us.app.viayoo.com	IP: 67.209.185.243 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052570 经度: -118.243904
www.baidu.com	IP: 110.242.68.4 所属国家: China 地区: Hebei 城市: Baoding 纬度: 38.851109 经度: 115.490280
play.google.com	IP: 172.217.160.78 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
	IP: 210.57.59.56

easylist-downloads.adblockplus.org	所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
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
saucenao.com	IP: 104.26.1.232 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
search.yahoo.com	IP: 108.160.166.253 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.bing.com	IP: 202.89.233.100 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
startpage.com	IP: 199.96.62.21 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
	IP: 112.84.222.56

beian.miit.gov.cn	所属国家: China 地区: Jiangsu 城市: Huai'an 纬度: 33.588612 经度: 119.019173
translate.google.com	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.yandex.ru	IP: 5.255.255.77 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
lingva.retiolus.net	IP: 65.21.91.32 所属国家: Finland 地区: Uusimaa 城市: Helsinki 纬度: 60.169521 经度: 24.935450

URL线索

URL信息	Url所在文件
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/bz.java
https://cfg.flurry.com/sdk/v1/config	d/b/b/c1.java
https://data.flurry.com/aap.do	d/b/b/m0.java

https://data.flurry.com/v1/flr.do	d/b/b/n0.java
https://easylist-downloads.adblockplus.org/easylist.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/Liste_AR.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/bulgarian_list.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easylistczechslovak.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_6_German/filter.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_9_Spanish/filter.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_16_French/filter.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/indianlist.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/abpindo.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easylistitaly.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/israellist.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_7_Japanese/filter.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/koreanlist.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easylistlithuania.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/latvianlist.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FiltersRegistry/master/filters/filter_8_Dutch/filter.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easylistpolish.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/rolist.txt	d/h/c/d/c.java

https://raw.githubusercontent.com/AdguardTeam/FilterRegistry/master/filters/filter_1_Russian/filter.txt	d/h/c/d/c.java
https://raw.githubusercontent.com/AdguardTeam/FilterRegistry/master/filters/filter_13_Turkish/filter.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/abpvn.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easylistchina.txt	d/h/c/d/c.java
https://fastly.jsdelivrivr.net/gh/cjx82630/cjxlist/cjx-annoyance.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/easyprivacy.txt	d/h/c/d/c.java
https://easylist-downloads.adblockplus.org/antiadblockfilters.txt	d/h/c/d/c.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	f/a/a/b/b.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	f/a/a/b/p.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	f/a/a/b/g.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	f/a/a/b/k.java
https://violentmonkey.github.io/api/gm/	h/a/b0/p0.java
https://viayoo.com/\n/	h/a/b0/p0.java
https://*/*\n/	h/a/b0/p0.java
https://*/*	h/a/b0/p0.java
https://github.com/tuyafeng/Via	h/a/h0/b4.java
http://viayoo.com/contact/telegram/	h/a/h0/b4.java
http://viayoo.com/contact/telegram-zh/	h/a/h0/b4.java

http://viayoo.com/contact/qqgroup/	h/a/h0/b4.java
https://twitter.com/tuyafeng	h/a/h0/b4.java
https://weibo.com/u/7558014976	h/a/h0/b4.java
http://viayoo.com/contact/wechat/	h/a/h0/b4.java
https://support.qq.com/product/438363	h/a/h0/b4.java
https://beian.miit.gov.cn/	h/a/h0/b4.java
https://github.com/androidx/androidx	h/a/h0/m4.java
https://github.com/google/dagger	h/a/h0/m4.java
https://github.com/ReactiveX/RxJava	h/a/h0/m4.java
https://github.com/ReactiveX/RxAndroid	h/a/h0/m4.java
https://github.com/uber/AutoDispose	h/a/h0/m4.java
https://github.com/square/okhttp	h/a/h0/m4.java
https://github.com/square/leakcanary/	h/a/h0/m4.java
https://github.com/shwenzhang/AndResGuard	h/a/h0/m4.java
https://github.com/Tencent/VasDolly	h/a/h0/m4.java
https://github.com/JakeWharton/timber	h/a/h0/m4.java
https://github.com/promeg/TinyPinyin	h/a/h0/m4.java
https://github.com/zxing/zxing	h/a/h0/m4.java
https://github.com/rburgst/okhttp-digest	h/a/h0/m4.java

https://github.com/thegrizzlylabs/sardine-android	h/a/h0/m4.java
https://file-examples.com/wp-content/uploads/2017/04/file_example_MP4_480_1_5MG.mp4	h/a/h0/i4.java
https://dav.jianguoyun.com/dav/	h/a/j0/p/l.java
https://help.eyeo.com/en/adblockplus/how-to-write-filters	h/a/r/m0.java
http://viayoo.com/	h/a/s/u2.java
http://viayoo.com/	h/a/t/v5.java
https://app.viayoo.com/addons/	h/a/t/t5.java
https://www.bing.com/images/searchbyimage?cbir=sbi&iss=sbi&imgurl=	h/a/t/t5.java
https://tineye.com/search/?url=	h/a/t/t5.java
https://yandex.com/images/touch/search?family=yes&rpt=imageview&url=	h/a/t/t5.java
http://st.so.com/stu?imgurl=	h/a/t/t5.java
https://saucenao.com/search.php?db=999&url=	h/a/t/t5.java
https://iqdb.org/?url=	h/a/t/t5.java
https://3d.iqdb.org/?url=	h/a/t/t5.java
https://trace.moe/?url=	h/a/t/t5.java
https://ascii2d.net/search/url/	h/a/t/t5.java
https://lens.google.com/uploadbyurl?url=	h/a/t/t5.java
https://fanyi.baidu.com/transpage?query=	h/a/t/t5.java

http://webtrans.yodao.com/webTransPc/index.html	h/a/t/t5.java
https://translate.google.com/translate?sl=auto&tl=	h/a/t/t5.java
https://m.baidu.com/?tn=&from=1022560v	h/a/u/k/a.java
https://www.google.com/	h/a/u/k/a.java
https://translate.google.com/translate_a/element.js?cb=googleTranslateElementInit\	h/a/u/k/b.java
https://www.google.com/images/clear.dot.gif	h/a/u/t/c.java
https://www.gstatic.com/images/branding/googlelogo/1x/googlelogo_color_68x28dp.png	h/a/u/t/c.java
https://res.viayoo.com/v1/latest_play.json	h/a/u/v/i.java
https://res.viayoo.com/v1/latest_cn.json	h/a/u/v/i.java
http://coolapk.com/apk/	h/a/u/w/y.java
https://play.google.com/store/apps/details?id=	h/a/u/w/y.java
http://viayoo.com/\	h/a/w/i/d.java
http://viayoo.com/contact/qqgroup/\	h/a/w/i/d.java
https://t.me/viatg\	h/a/w/i/d.java
https://github.com/tuyafeng/Via\	h/a/w/i/d.java
https://www.google.com/search?q=	h/a/w/j/k.java
https://www.bing.com/search?q=	h/a/w/l/b.java
https://m.baidu.com/s?word=	h/a/w/l/a.java

https://m.baidu.com/s?from=	h/a/w/l/a.java
https://www.baidu.com/s?word=	h/a/w/l/a.java
https://www.baidu.com/s?from=	h/a/w/l/a.java
https://duckduckgo.com/?q=	h/a/w/l/d.java
https://www.google.com/search?q=	h/a/w/l/e.java
https://m.so.com/s?q=	h/a/w/l/f.java
https://www.so.com/s?q=	h/a/w/l/f.java
https://startpage.com/do/search?query=	h/a/w/l/j.java
https://wap.sogou.com/web/sl?keyword=	h/a/w/l/i.java
https://wap.sogou.com/web/sl?bid=sogou-mobb-	h/a/w/l/i.java
https://www.sogou.com/web?query=	h/a/w/l/i.java
https://yz.m.sm.cn/s?q=	h/a/w/l/h.java
https://yz.m.sm.cn/s?from=	h/a/w/l/h.java
https://so.toutiao.com/search/?keyword=	h/a/w/l/k.java
https://so.toutiao.com/search?keyword=%@	h/a/w/l/k.java
https://search.yahoo.com/search?p=	h/a/w/l/l.java
https://www.yandex.ru/search/touch/?text=	h/a/w/l/m.java
https://yandex.ru/search/?text=	h/a/w/l/m.java
https://app.viayoo.com/api/user?	h/a/w/m/a.java

https://viayoo.com/zh-cn/docs/terms-of-use.html	h/a/w/m/a.java
https://app.viayoo.com/api/update	h/a/w/m/a.java
https://viayoo.com/zh-cn/docs/privacy-policy.html	h/a/w/m/a.java
https://app.viayoo.com/api/sync?	h/a/w/m/a.java
https://us.app.viayoo.com/api/user?	h/a/w/m/b.java
https://viayoo.com/en/docs/terms-of-use.html	h/a/w/m/b.java
https://us.app.viayoo.com/api/update	h/a/w/m/b.java
https://viayoo.com/en/docs/privacy-policy.html	h/a/w/m/b.java
https://us.app.viayoo.com/api/sync?	h/a/w/m/b.java
https://viayoo.com/	h/a/w/o/e/d.java
https://app.viayoo.com/addons/	h/a/w/o/e/d.java
https://sug.so.360.cn/suggest?encodein=utf-8&encodeout=utf-8&format=json&word=	h/a/w/p/i/d.java
https://clients1.google.com/complete/search?hl=	h/a/w/p/i/c.java
https://api.bing.com/qsm1.aspx?market=	h/a/w/p/i/b.java
https://suggestion.baidu.com/su?wd=	h/a/w/p/i/a.java
https://lingva.retiolus.net/api/v1/	h/a/w/q/a.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/rxjava3/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/rxjava3/exceptions/UndeliverableException.java

https://my.cdn.com/jquery.js</tt>.	Mogua Engine V1
https://www.google.com/something	Mogua Engine V1
https://www.google.com/any/*	Mogua Engine V1
https://www.google.com/any/not_me	Mogua Engine V1
https://my.cdn.com/jquery.js</tt>	Mogua Engine V1

 邮箱线索

邮箱地址	所在文件
yafengtu@gmail.com	h/a/h0/b4.java
yafengtu@gmail.com	h/a/h0/f4.java
2376688759@qq.com wiar1824@gmail.com	h/a/w/i/d.java
2376688759@qq.com wiar1824@gmail.com	Mogua Engine V1

 手机线索

 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=CN, ST=广西, L=广西, CN=Various Tu
签名算法: rsassa_pkcs1v15
有效期自: 2014-08-27 05:03:28+00:00
有效期至: 2114-08-03 05:03:28+00:00
发行人: C=CN, ST=广西, L=广西, CN=Various Tu
序列号: 0x3f3b121a
哈希算法: sha256
md5值: 9830874658327c15600f6e4ea939c324
sha1值: af5d11b1703127167e23b45fa706f0dd9865499b
sha256值: 3df7f89d3b8d1315f05710c914fccbcf3a4e24980afddccb8dcebd90836a390
sha512值: a1325fe5ee670753629e4741a6492684f9f06d54660e51d9facfd086fcae18a3399eae57b63038dfd3b7d70c6b90be91787cb229f0c71541e9427a17a23fbe22
公钥算法: rsa
密钥长度: 2048
指纹: b59491fe7b82fd23aedec96f9b1f35082a50bf5a21b4e952543b75780193986b

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
mark.via.permission.BROADCAST	未知	Unknown permission	Unknown permission from android reference
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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
android.permission.POST_NOTIFICATIONS	未知	Unknown permission	Unknown permission from android reference
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
android.permission.MODIFY_AUDIO_SETTINGS	正常	更改您的音频设置	允许应用程序修改全局音频设置,例如音量和路由

com.android.launcher.permission.INSTALL_SHORTCUT	未知	Unknown permission	Unknown permission from android reference
com.bbk.launcher2.permission.READ_SETTINGS	未知	Unknown permission	Unknown permission from android reference
com.google.android.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
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

应用内通信

活动(ACTIVITY)	通信(INTENT)
mark.via.Shell	Schemes: http://, https://, about://, javascript://, inline://, file://, content://, Mime Types: text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml,