



MoGua

铁粉空间 1.1.1.APK 分析报告



APP名称:

铁粉空间

包名: com.tfkjppx.tfkj025784212348dfsd

域名线索: 43条

URL线索: 19条

邮箱线索: 3条

分析日期: 2025年6月21日

分析平台: [摸瓜APK反编译平台](#)

文件名: 铁粉空间.apk
文件大小: 23.63MB
MD5值: 81296f8e9c85435e1b9da76ea87a222c
SHA1值: 829562048f1158d94fc74c1cd01d8f7a8f2f2c51
SHA256值: 39119b46fb87750d1abab9bf0e23318e13d37a6faa4219ede510d9f8a13c001b

i APP 信息

App名称: 铁粉空间
包名: com.tfkjppx.tfkj025784212348dfsd
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
cdn.jsdelivr.net	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
swiperjs.comn	没有服务器地理信息.
img01.yzcdn.cn	IP: 202.108.29.158 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 34.92.14.65

34.92.14.65	所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
douyin-api.ybunx.com	IP: 172.67.139.69 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
faw.douying8.com	没有服务器地理信息.
d1tlfquc8pdvcm.cloudfront.net	IP: 13.33.47.228 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
axios-http.com	IP: 52.74.232.59 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
i.ytimg.com	IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires

	城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
www.youtube.com	IP: 31.13.73.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249
jsperf.com	IP: 104.16.227.18 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
raw.githubusercontent.com	IP: 185.199.108.133 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724
aomedia.org	IP: 162.125.32.5 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
player.vimeo.com	IP: 31.13.94.36 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
	IP: 172.67.140.170

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
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
hfive.qsxon.com	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
brianleroux.github.com	没有服务器地理信息.
noembed.com	IP: 151.101.193.91 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
npms.io	IP: 104.21.112.1 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: 199.16.158.9 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
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
go.aniview.com	IP: 104.83.102.21 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
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
ii.tqj655.com	IP: 118.107.9.190 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
	IP: 104.26.13.19 所属国家: United States of America

cdn.plyr.io	地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
html2canvas.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
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
baq.fbafb.cn	没有服务器地理信息.
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
18.167.82.135	IP: 18.167.82.135 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
bird.ile789.com	IP: 118.107.9.190 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong

	纬度: 22.285521 经度: 114.157692
schemas.android.com	没有服务器地理信息.
cres.rqi564.com	IP: 149.104.35.195 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
dfe.hapha.cn	没有服务器地理信息.
ldy.nroom10.com	没有服务器地理信息.
bought.vgm849.com	IP: 104.21.32.1 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
api.h-gpro.com	没有服务器地理信息.
vimeo.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
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

chen.ybunx.com	IP: 172.67.139.69 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://chen.ybunx.com/apk/app-1.1.0-3.apk	defpackage/j00.java
https://dfe.hapha.cn	defpackage/l00.java
https://api.h-gpro.com	defpackage/l00.java
https://baq.fbafb.cn	defpackage/l00.java
https://faw.douying8.com	defpackage/l00.java
https://douyin-api.ybunx.com	defpackage/l00.java
http://schemas.android.com/apk/res/android	defpackage/b0.java
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
https://cdn.jsdelivr.net/npm/workbox-cdn@5.1.4/workbox	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://t.me/\$	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://d1tlfquc8pdvcm.cloudfront.net/api/v1/	摸瓜V2引擎
https://bought.vgm849.com/api/v1	摸瓜V2引擎
https://bird.ile789.com/api/v1	摸瓜V2引擎
https://ii.tqj655.com/api/v1/	摸瓜V2引擎
https://34.92.14.65:18888/api/v1/	摸瓜V2引擎
https://18.167.82.135:18888/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://npms.io/search?q=ponyfill.	摸瓜V2引擎
https://github.com/zloirock/core-js/blob/v3.39.0/LICENSE	摸瓜V2引擎
https://github.com/zloirock/core-js	摸瓜V2引擎
https://a	摸瓜V2引擎
https://a/c%20d?a=1&c=3	摸瓜V2引擎
https://a@b	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://raw.githubusercontent.com/stefanpenner/es6-promise/master/LICENSE	摸瓜V2引擎

邮箱线索

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

手机线索

手机号	所在文件
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: 2025-06-07 07:09:26+00:00
有效期至: 2052-10-23 07:09:26+00:00
发行人: C=xx, ST=xx, L=xx, O=XX, OU=xx, CN=xx.com
序列号: 0x3186abcd
哈希算法: sha256
md5值: 6b760a19e10d00c60925dc3f0625de95
sha1值: fbeabda5cff8e836bb58bf9b454900bd41deab5d
sha256值: 9a86af36c3fcebe5cf4ac75d963db5d3ff535b6c89c6f1c8d7bb6356bd923208
sha512值: 54258ab2e7e2038b96c048c6934dbcb138aa01cee1579a3abe686ad7c64be65038ffd4f5033fa0f1a74900a060ff9b034614206a66e40e220aa9265cc5d4528b
公钥算法: rsa
密钥长度: 2048
指纹: fc8d1af3f5c7dfa891b2ff0fd9b7681a6d74952f71cf1371d4dcbc7998329ab4

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