



MoGua

KF6.VIP 5.APK 分析报告



APP名称:

KF6.VIP

包名:	com.ytfde.ufes
域名线索:	30条
URL线索:	42条
邮箱线索:	1条
分析日期:	2025年6月28日
分析平台:	摸瓜APK反编译平台

文件名: APP16422025062301.apk
文件大小: 78.76MB
MD5值: 757cf3d234d8e391190e118e409350fb
SHA1值: 7939c855ed3f58d0d16377b9eaf9cd65919e6333
SHA256值: d38171dc5e34fba1847273f5a58a658a88bf48724757dafe89ea4f5e7f975777

i APP 信息

App名称: KF6.VIP
包名: com.ytfde.ufes
主活动Activity: com.game.main.MainActivity
安卓版本名称: 5
安卓版本: 5

🔍 域名线索

域名	服务器信息
developer.umeng.com	IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
www.softwareishard.com	IP: 91.239.200.59 所属国家: Czechia 地区: Praha, Hlavni mesto 城市: Prague 纬度: 50.087936 经度: 14.420798
cocos2d-x.org	IP: 54.241.49.5 所属国家: United States of America 地区: California

	城市: San Jose 纬度: 37.339390 经度: -121.894958
alogsus.umeng.com	IP: 223.109.148.176 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
www.68chat.com	IP: 47.83.118.180 所属国家: United States of America 地区: California 城市: San Mateo 纬度: 37.547424 经度: -122.330589
getfirebug.com	IP: 3.33.186.135 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.627499 经度: -122.346199
zhcsuat.cdnvips.net	IP: 104.26.15.69 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
plbslog.umeng.com	IP: 36.156.202.75 所属国家: China 地区: Jiangsu 城市: Yangzhou 纬度: 32.397221 经度: 119.435600
	IP: 114.117.133.42

new-api.meiqia.com	所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
www.khronos.org	IP: 159.65.181.57 所属国家: United States of America 地区: New Jersey 城市: Clifton 纬度: 40.858585 经度: -74.163605
reportlog.cocos.com	IP: 39.97.6.35 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
ulogs.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
example.com	IP: 23.215.0.136 所属国家: Australia 地区: New South Wales 城市: Sydney 纬度: -33.867779 经度: 151.207047
incompleteness.me	IP: 35.185.44.232 所属国家: United States of America 地区: South Carolina 城市: North Charleston 纬度: 32.888702

	经度: -80.007584
alogus.umeng.com	IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
meiqia.com	IP: 114.117.133.42 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
notify.bugsnag.com	IP: 35.186.205.6 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
ulogs.umengcloud.com	IP: 223.109.148.177 所属国家: China 地区: Jiangsu 城市: Nanjing 纬度: 32.061668 经度: 118.777992
182.92.20.189	IP: 182.92.20.189 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
	IP: 203.119.145.40 所属国家: China

cmnsguider.yunos.com	地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tsis.jpush.cn	IP: 123.60.218.46 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
getline.csaabx.com	IP: 104.21.6.78 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mozilla.org	IP: 35.190.14.201 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
dxr.mozilla.org	IP: 35.190.14.201 所属国家: United States of America 地区: Missouri 城市: Kansas City 纬度: 39.099731 经度: -94.578568
long.open.weixin.qq.com	IP: 112.65.193.170 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948

ejohn.org	IP: 44.230.85.241 所属国家: United States of America 地区: Oregon 城市: Portland 纬度: 45.523460 经度: -122.676468
ouplog.umeng.com	IP: 47.246.110.94 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
hg.mozilla.org	IP: 63.245.208.203 所属国家: United States of America 地区: California 城市: Palo Alto 纬度: 37.444057 经度: -122.160225
open.weixin.qq.com	IP: 116.128.171.214 所属国家: China 地区: Shanghai 城市: Shanghai 纬度: 31.224333 经度: 121.468948
www.cocos2d-x.org	IP: 54.241.49.5 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958

URL信息	Url所在文件
http://182.92.20.189:9099/	cn/jiguang/a/a/c/i.java
https://tsis.jpush.cn	cn/jiguang/c/a.java
https://new-api.meiqia.com/client/send_msg	com/meiqia/core/d.java
https://new-api.meiqia.com/client/send_msg	com/meiqia/core/h.java
https://new-api.meiqia.com/knowledge/questions/	com/meiqia/core/h.java
https://new-api.meiqia.com/client/file_downloaded	com/meiqia/core/h.java
https://new-api.meiqia.com/client/tickets_v2/	com/meiqia/core/h.java
https://new-api.meiqia.com/client/msg_delivered	com/meiqia/core/h.java
https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass_message_receipts	com/meiqia/core/h.java
https://new-api.meiqia.com/client/end_conversation	com/meiqia/core/h.java
https://new-api.meiqia.com/client/queue/position	com/meiqia/core/h.java
https://new-api.meiqia.com/client/tickets_v2/categories	com/meiqia/core/h.java
https://new-api.meiqia.com/upload?user_id=	com/meiqia/core/h.java
https://new-api.meiqia.com/upload/oss/policies	com/meiqia/core/h.java
https://new-api.meiqia.com/client/inputting	com/meiqia/core/h.java
https://new-api.meiqia.com/conversation/	com/meiqia/core/h.java
https://new-api.meiqia.com/sdk/init_sdk_user	com/meiqia/core/h.java

https://new-api.meiqia.com/client/device_token	com/meiqia/core/h.java
https://new-api.meiqia.com/client/prechat-survey-msg	com/meiqia/core/h.java
https://new-api.meiqia.com/unified-api/conversations/v1/client/unreceived_mass_messages	com/meiqia/core/h.java
https://new-api.meiqia.com/sdk/statistics	com/meiqia/core/h.java
https://new-api.meiqia.com/client/forms	com/meiqia/core/h.java
https://new-api.meiqia.com/client/attrs	com/meiqia/core/h.java
https://new-api.meiqia.com/client/	com/meiqia/core/h.java
https://new-api.meiqia.com/scheduler	com/meiqia/core/h.java
https://new-api.meiqia.com/sdk/init	com/meiqia/core/h.java
https://new-api.meiqia.com/client/tickets_v2	com/meiqia/core/h.java
https://new-api.meiqia.com/client/tickets	com/meiqia/core/h.java
https://new-api.meiqia.com/client/msg_read	com/meiqia/core/h.java
https://new-api.meiqia.com/unified-api/conversations/v1/client/sdk/mass_messages/	com/meiqia/core/h.java
https://new-api.meiqia.com/sdk/get_dev_client_id	com/meiqia/core/h.java
https://new-api.meiqia.com/sdk/refresh_push_info	com/meiqia/core/h.java
https://new-api.meiqia.com/client/client_events	com/meiqia/core/h.java
https://new-api.meiqia.com/mpush/copy/statistics	com/meiqia/core/h.java

https://notify.bugsnag.com	com/meiqia/core/a/e.java
http://meiqia.com/	com/meiqia/core/a/e.java
https://new-api.meiqia.com/captchas	com/meiqia/meiqiasdk/util/HttpUtils.java
https://new-api.meiqia.com	com/meiqia/meiqiasdk/util/HttpUtils.java
https://reportlog.cocos.com	com/cocos/analytics/c/c.java
https://getline.csaabbx.com/?m=	com/example/mylibrary/ServiceActivity.java
https://zhcsuat.cdnvips.net/index/index/getKefuInfo?kefuCode=	com/example/mylibrary/ServiceActivity.java
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s	com/tencent/mm/opensdk/diffdev/a/c.java
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s×tamp=%s&scope=%s&signature=%s	com/tencent/mm/opensdk/diffdev/a/b.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com/unify_logs	com/umeng/commonsdk/statistics/UMServerURL.java
https://cmnsguider.yunos.com:443/genDeviceToken	com/umeng/commonsdk/statistics/idtracking/s.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java

http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/h.java
http://example.com/	cz/msebera/android/httpclient/impl/client/cache/CacheKeyGenerator.java
http://cocos2d-x.org	摸瓜V2引擎
https://hg.mozilla.org/mozilla-central/file/d1c70c20e7b5/addon-sdk/source/lib/sdk/	摸瓜V2引擎
http://www.khronos.org/registry/webgl/specs/latest/webgl.idl	摸瓜V2引擎
http://ejohn.org/	摸瓜V2引擎
http://www.cocos2d-x.org/docs/manual/framework/html5/v3/reflection/en	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://www.softwareishard.com/blog/firebug/nsitraceablechannel-intercept-http-traffic/	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
https://dxr.mozilla.org/webtools-central/source/tbpl/php/inc/GeneralErrorFilter.php	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://getfirebug.com/wiki/index.php/Command_Line_API	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎

http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://incompleteness.me/blog/2015/02/09/console-dot-mihai/	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://mozilla.org/MPL/2.0/.	摸瓜V2引擎
http://www.cocos2d-x.org/docs/manual/framework/html5/v3/assets-manager/en	摸瓜V2引擎
https://www.68chat.com	摸瓜V2引擎

 邮箱线索

邮箱地址	所在文件
ze@z.fr ly@phm.1tw 0@t6ycp.8kqu 84nt@i.3r 1d@4p.u³ee	摸瓜V2引擎

手机线索

签名证书

APK已签名
v1 签名: True
v2 签名: False
v3 签名: False
找到 1 个唯一证书
主题: C=fed, ST=fevd, L=fde, O=fad, OU=fedc, CN=fdddw
签名算法: rsassa_pkcs1v15
有效期自: 2021-06-08 10:45:00+00:00
有效期至: 2076-03-11 10:45:00+00:00
发行人: C=fed, ST=fevd, L=fde, O=fad, OU=fedc, CN=fdddw
序列号: 0x1b47a23d
哈希算法: sha256
md5值: ba917aea6ec1a0a9a668c9d7074e3989
sha1值: 1653cc3d16e2f047c074fa7b9aeaaa86135c7c3f
sha256值: 8fd4b27c0fa506a064dd77eeb23254071072b3db86002c9291d51eda07727b1e
sha512值: 8f8764d269489b10ef029afeef12a06d14f412c9509f1d9ac1d9877079d16f8616816d7d54188fbba89a62c1e35b6e44bb990f2f7d27e9bc66db4cfd2d4aa6d8

硬编码敏感信息

可能的敏感信息

"cancel_auth" : "取消登录"
"get_token_from_weixin" : "获取微信访问Token"
"mq_auth_code" : "验证码"
"target_scene_session" : "会话"
"mq_auth_code" : "CAPTCHA"
"mq_auth_code" : "Kode verifikasi"
"mq_auth_code" : "Kod pengesahan"
"mq_auth_code" : "驗證碼"

 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.CHANGE_NETWORK_STATE	正常	更改网络连接	允许应用程序更改网络连接状态。
android.permission.CHANGE_WIFI_STATE	正常	更改Wi-Fi状态	允许应用程序连接和断开 Wi-Fi 接入点,并对配置的 Wi-Fi 网络进行更改
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.READ_PHONE_STATE	危险	读取电话状态和身份	允许应用访问设备的电话功能。具有此权限的应用程序可以确定此电话的电话号码和序列号,呼叫是否处于活动状态,呼叫所连接的号码等
android.permission.READ_PRIVILEGED_PHONE_STATE	未知	Unknown permission	Unknown permission from android reference
android.permission.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统
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.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低

android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BLUETOOTH_ADMIN	正常	蓝牙管理	允许应用程序发现和配对蓝牙设备。
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
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
com.ytfde.ufes.permission.JPUSH_MESSAGE	未知	Unknown permission	Unknown permission from android reference
android.permission.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置
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.ACCESS_LOCATION_EXTRA_COMMANDS	正常	访问额外的位置提供程序命令	访问额外的位置提供程序命令，恶意应用程序可能会使用它来干扰 GPS 或其他位置源的操作

应用内通信

活动(ACTIVITY)	通信(INTENT)
com.game.main.MainActivity	Schemes: obofmp://,

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。