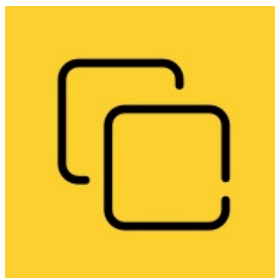




MoGua

幻影分身 4.1.8.APK 分析报告



APP名称:

幻影分身

包名:	com.hy.clone
域名线索:	26条
URL线索:	3条
邮箱线索:	1条
分析日期:	2025年7月3日
分析平台:	摸瓜APK反编译平台

文件名: 幻影分身.apk
文件大小: 35.54MB
MD5值: 56f934c3a27250719c9a990732f042b7
SHA1值: 942da9ef6eaace842afb509cd25bcea869a7d079
SHA256值: d027c48077ad7f04950fd74c41636c60e4a765e27946a6ea98eb17c90f7dcb08

i APP 信息

App名称: 幻影分身
包名: com.hy.clone
主活动Activity: io.qihoo.splash.SplashActivity
安卓版本名称: 4.1.8
安卓版本: 418

🔍 域名线索

域名	服务器信息
log.snssdk.com	IP: 42.236.86.168 所属国家: China 地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
applog.snssdk.com	IP: 42.56.93.208 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
	IP: 123.126.74.239 所属国家: China 地区: Beijing

sf1-amtos-cdn.bytesmanager.com	城市: Beijing 纬度: 39.907501 经度: 116.397102
ad.zijieapi.com	IP: 111.161.204.209 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
gcc.gnu.org	IP: 8.43.85.97 所属国家: United States of America 地区: North Carolina 城市: Raleigh 纬度: 35.773994 经度: -78.632759
ad.oceanengine.com	IP: 42.56.93.207 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
connectivitycheck.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
mps.amap.com	IP: 59.82.113.71 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583

sf16-static.i18n-pglstatp.com	IP: 23.220.70.35 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
apmlog.snssdk.com	IP: 116.196.143.217 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
sf3-fe-tos.pglstatp-toutiao.com	IP: 101.73.101.3 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041599 经度: 114.478081
hyapps.huanyings.com	IP: 61.48.83.205 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
toblog.ctobsnssdk.com	IP: 111.161.204.210 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142181 经度: 117.176102
api-access.pangolin-sdk-toutiao.com	IP: 42.56.65.94 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221

	经度: 123.432877
www.pangle.cn	IP: 116.196.143.221 所属国家: China 地区: Zhejiang 城市: Jinhua 纬度: 30.013470 经度: 120.288658
tobapplog.ctobsnssdk.com	IP: 42.56.93.212 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
maps.testing.amap.com	IP: 59.82.57.204 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
ichannel.snssdk.com	IP: 221.204.58.138 所属国家: China 地区: Shanxi 城市: Taiyuan 纬度: 37.869438 经度: 112.561508
rtapplog.snssdk.com	IP: 119.188.50.35 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223
	IP: 42.236.86.168 所属国家: China

playable.oceanengine.com	地区: Henan 城市: Zhengzhou 纬度: 34.757778 经度: 113.648613
success.ctobsnssdk.com	IP: 139.215.162.53 所属国家: China 地区: Jilin 城市: Changchun 纬度: 43.880001 经度: 125.322777
m5.amap.com	IP: 59.82.113.187 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161583
rtlog.snssdk.com	IP: 42.56.93.211 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432877
www.huanyings.com	IP: 61.48.83.207 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
mpsapi.amap.com	IP: 106.11.43.68 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102

127.0.0.1	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
-----------	--

 URL线索

URL信息	Url所在文件
http://www.huanyings.com	摸瓜V1引擎
http://hyapps.huanyings.com	摸瓜V1引擎
https://sf1-amtos-cdn.bytesmanager.com/obj/ad-app-package/personal-privacy-page.html	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
clientservices.googleapis.com	摸瓜V3引擎
https://success.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/abtest_config/	摸瓜V3引擎
http://127.0.0.1	摸瓜V3引擎
https://ad.oceanengine.com/track/activate/	摸瓜V3引擎
https://rtlog.snssdk.com/service/2/app_log/	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎

https://api-access.pangolin-sdk-toutiao.com/v2/inspect/aegis/client/page/	摸瓜V3引擎
gmscompliance-pa.googleapis.com	摸瓜V3引擎
connectivitycheck.gstatic.com	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/app_alert_check/	摸瓜V3引擎
https://apmlog.snssdk.com/apm/collect/crash/	摸瓜V3引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/ttfe/adfe/union_endcard/Lark20190725-175511.png	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/device_register_only/	摸瓜V3引擎
https://tobapplog.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://rtapplog.snssdk.com/service/2/app_log/	摸瓜V3引擎
https://sf3-fe-tos.pglstatp-toutiao.com/obj/ad-pattern/renderer/package.json	摸瓜V3引擎
android.googleapis.com	摸瓜V3引擎
http://gcc.gnu.org/bugs.html :	摸瓜V3引擎
https://ichannel.snssdk.com/service/2/app_alert_check/	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/log_settings/	摸瓜V3引擎
https://log.snssdk.com/service/2/log_settings/	摸瓜V3引擎
https://log.snssdk.com/service/2/device_register_only/	摸瓜V3引擎
https://playable.oceanengine.com/web-api/v1/coldstart	摸瓜V3引擎

https://www.pangle.cn/privacy/partner	摸瓜V3引擎
https://api-access.pangolin-sdk-toutiao.com	摸瓜V3引擎
https://applog.snssdk.com/service/2/app_log/	摸瓜V3引擎
https://toblog.ctobsnssdk.com/service/2/app_log/	摸瓜V3引擎
https://ad.zijieapi.com/api/ad/v1/aggregate/search_lu	摸瓜V3引擎
https://sf16-static.i18n-pglstatp.com/obj/ad-pattern-sg/static/images/	摸瓜V3引擎
https://log.snssdk.com/service/2/app_log/	摸瓜V3引擎
http://mpsapi.amap.com/ws/mps/vmap/	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://mpsapi.amap.com/ws/mps/rtt/	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://mpsapi.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://m5.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://mpsapi.amap.com/ws/mps/lyrdata/ugc/	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://mpsapi.amap.com/	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
http://m5.amap.com	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
https://mps.amap.com/ws/mps/rtt	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
https://mps.amap.com/ws/mps/vmap	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
https://maps.testing.amap.com/ws/transfer/auth/map/indoor_maps	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so

https://mps.amap.com/ws/mps/smap	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
https://mps.amap.com/ws/mps/spot	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so
https://mps.amap.com/ws/mps/hot	lib/arm64-v8a/libAMapSDK_MAP_v9_7_0.so

邮箱线索

邮箱地址	所在文件
发送到邮件huan90s@163.com	摸瓜V1引擎

手机线索

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=QD, ST=山东省, L=青岛市, O=海尔, OU=中国, CN=Huan
签名算法: rsassa_pkcs1v15
有效期自: 2018-12-15 11:47:04+00:00
有效期至: 2117-11-21 11:47:04+00:00
发行人: C=QD, ST=山东省, L=青岛市, O=海尔, OU=中国, CN=Huan
序列号: 0x6378bf70
哈希算法: sha256
md5值: a1ccb0d670efba1bc4353b1bc8ddf4f7
sha1值: f60eda7015da4c0e4d7b72a0bc509df7cd16429f
sha256值: 73d839943f868bd049f21ce6d96cff1dafab7e0e2d47d37e47b59fd06856b1cc
sha512值: d7dd8aa40f5bb099b50aaaa106beab45f1c1e7441b62ba89065a5b8b90db4306f9e51afd6f3fc0abbfa14b06678892878726eb1b4e26c7fb755fcde53e104dfe

公钥算法: rsa
密钥长度: 2048
指纹: 84e3ac84eeff5f677342d6d168c39101797aa5c72af5353ff65b859438dbe361

硬编码敏感信息

可能的敏感信息
"get_wxtoken_tip" : "1.可通过抓包工具获取微信小程序“捉妖雷达”的身份码，填写后即可共享。 2.年费用户共享成功一次，可以获得1天VIP时间奖励。 3.普通用户共享成功一次，可以获得两小时的雷达使用时间。 4.身份码获取方法可进入售后群或者王者群查看"
"google_maps_key" : "AlzaSyDBMDDx4Yz7SNCm_Kq6MRZiKEGdapFfU44"
"input_pwd" : "请输入密码"
"share_wxtoken" : "填写身份码"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"token_expire" : "登录token过期或账号已在其他设备登录，请重新登录。"
"smssdk_authorize_dialog_accept" : "同意"
"smssdk_authorize_dialog_reject" : "拒绝"
"smssdk_authorize_dialog_title" : "服务授权"
"smssdk_authorize_dialog_accept" : "Agree"
"smssdk_authorize_dialog_reject" : "Disagree"

"smssdk_authorize_dialog_title" : "Terms of Use"
"get_wxtoken_tip" : "1.可通过抓包工具获取微信小程序“捉妖雷达”的身份码，填写后即可共享。 2.年费用户共享成功一次，可以获得1天VIP时间奖励。 3.普通用户共享成功一次，可以获得两小时的雷达使用时间。 4.身份码获取方法可进入售后群或者王者群查看"
"input_pwd" : "请输入密码"
"share_wxtoken" : "填写身份码"
"token_expire" : "登录token过期或账号已在其他设备登录，请重新登录。"

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

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。