MoGua

火星农夫 1.0.2.APK 分析报告

APP名称:	火星农夫
包名:	com.sc.hxnf
域名线索:	33条
URL线索:	58条
邮箱线索:	0条
分析日期:	2024年4月20日
分析平台:	摸瓜反编译平台

文件信息

文件名: hxnf.apk
文件大小: 64.24MB
MD5值: 0625e51d9604aaece07187f1aab1f62f
SHA1值: bcea829cf429b3ac67812caa08e5e718383e8788
SHA256值: 1cadce4bc0671f194e3d656baa00f9c80e06dd86483f43752a6a50a3b0c39be2

APP 信息

App名称: 火星农夫
包名: com.sc.hxnf
主活动Activity: com.sc.hxnf.ui.activity.SplashActivity
安卓版本名称: 1.0.2
安卓版本: 2

域名线索

域名	服务器信息
github.com	**IP**: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
route.showapi.com	**IP**: 116.62.176.13 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
api.mch.weixin.qq.com	**IP**: 182.254.63.17 **所属国家**: China **地区**: Guangdong **城市**: Shenzhen **纬度**: 22.545540 **经度**: 114.068298

adiu.amap.com	**IP**: 59.82.31.100 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
image.cnamedomain.com	没有服务器地理信息.
cgicol.amap.com	**IP**: 59.82.31.99 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ku.cndesign.com	没有服务器地理信息.
oss-cn-.aliyuncs.comor	没有服务器地理信息.
cloudauth.cn-beijing.aliyuncs.com	**IP**: 101.201.182.3 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
dualstack-a.apilocate.amap.com	**IP**: 106.11.40.50 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
api.weixin.qq.com	**IP**: 109.244.145.152 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
mgw.mpaas.cn-hangzhou.aliyuncs.com	**IP**: 47.96.141.131 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
render.alipay.com	**IP**: 220.181.135.244 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
apilocate.amap.com	**IP**: 59.82.31.183 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 106.11.61.111

cloudauth-dualstack.aliyuncs.com	**所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
abroad.apilocate.amap.com	IP: 59.82.44.11 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
restsdk.amap.com	IP: 203.119.175.194 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
ic.snssdk.com	IP: 42.81.213.228 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142220 **经度**: 117.176666
lbs.amap.com	IP: 59.82.29.231 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
oss.aliyuncs.com	IP: 118.178.29.5 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
hxnf.xingpingshicai.cn	IP: 118.190.154.195 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
cloudauth.aliyuncs.com	IP: 140.205.174.3 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
uri.amap.com	IP: 203.119.214.251 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
	IP: 39.98.22.142 **所属国家**: China

dualstack-arestapi.amap.com	**地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
long.open.weixin.qq.com	IP: 109.244.216.15 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
open.weixin.qq.com	IP: 109.244.144.48 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.acfun.tv	IP: 34.102.136.180 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
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
cloudauth-dualstack.cn-beijing.aliyuncs.com	IP: 182.92.29.46 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
oss-cn-hangzhou.aliyuncs.com	IP: 118.31.219.251 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161423
jandan.net	IP: 140.249.61.203 **所属国家**: China **地区**: Shandong **城市**: Qingdao **纬度**: 36.098610 **经度**: 120.371941
www.baidu.com	IP: 110.242.68.3 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
schemas.android.com	没有服务器地理信息.

URL线索

URL信息
https://render.alipay.com/p/f/fd-j8l9yjja/index.html
https://cloudauth-dualstack.aliyuncs.com
https://cloudauth-dualstack.cn-beijing.aliyuncs.com
https://cloudauth.aliyuncs.com
https://cloudauth.cn-beijing.aliyuncs.com
http://www.acfun.tv/
http://www.baidu.com/s?wd=
http://jandan.net/?oxwlxojflwblxbsapi=jandan.get_pic_comments&page=
http://ic.snssdk.com/neihan/stream/mix/v1/? mpic=1&essence=1&content_type=-102&message_cursor=-1&bd_Stringitude=113.369569&bd_latitude=23.149678&bd_city=%E5%B9%BF%E5%B7%9E%E5%B8%82&am_Stringitude=113.367846&am_latitude=23.149878&am_city=%E5%B9%BF%E5%B7%9E%E5%B8%82&am_loc_time=14
http://route.showapi.com/255-1?type=31&showapi_appid=20569&showapi_sign=0707a6bfb3e842fb8c8aa450012d9756&page=
http://ku.cndesign.com/pic/
http://jandan.net/?oxwlxojflwblxbsapi=jandan.get_ooxx_comments&page=
https://github.com/tamsiree/RxTool
https://api.mch.weixin.qq.com/pay/unifiedorder
www.baidu.com
http://uri.amap.com/navigation?to=
https://mgw.mpaas.cn-hangzhou.aliyuncs.com
https://hxnf.xingpingshicai.cn/register.html?spreadUid=
https://api.weixin.qq.com/sns/oauth2/access_token?appid=%s&secret=%s&code=%s&grant_type=authorization_code
https://adiu.amap.com/ws/device/adius
https://restsdk.amap.com/sdk/compliance/params
http://restsdk.amap.com/sdk/compliance/params
http://restsdk.amap.com
http://apilocate.amap.com/mobile/binary
http://dualstack-a.apilocate.amap.com/mobile/binary

http://abroad.apilocate.amap.com/mobile/binary
http://dualstack-arestapi.amap.com/v3/geocode/regeo
http://restsdk.amap.com/v3/geocode/regeo
http://cgicol.amap.com/collection/collectData?src=baseCol&ver=v74&
https://restsdk.amap.com/v3/iasdkauth
https://dualstack-arestapi.amap.com/v3/iasdkauth
http://abroad.apilocate.amap.com/mobile/binary
http://abroad.apilocate.amap.com/mobile/binary
http://restsdk.amap.com/v3/place/text?
http://restsdk.amap.com/v3/config/district?
http://restsdk.amap.com/v3/place/around?
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://open.weixin.qq.com/connect/sdk/qrconnect?appid=%s&noncestr=%s&timestamp=%s&scope=%s&signature=%s
https://long.open.weixin.qq.com/connect/l/qrconnect?f=json&uuid=%s
http://lbs.amap.com/api/android-location-sdk/guide/utilities/errorcode/查看错误码说明
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android
http://schemas.android.com/apk/res/android
https://hxnf.xingpingshicai.cn
https://ip.
http://oss-cn-****.aliyuncs.com',or
http://image.cnamedomain.com'!

http://oss.aliyuncs.com
http://127.0.0.1
http://oss-cn-****.aliyuncs.com',or
http://image.cnamedomain.com'!
http://oss-cn-hangzhou.aliyuncs.com
http://schemas.android.com/apk/res/android
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling
https://github.com/ReactiveX/RxJava/wiki/Error-Handling
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins

邮箱线索

手机线索

手机号	所在文件
17215021497	com/tamsiree/rxkit/RxConstants.java
15778800000	org/joda/time/chrono/JulianChronology.java
15778800000	org/joda/time/chrono/BasicFixedMonthChronology.java
15308640144	org/joda/time/chrono/IslamicChronology.java
15778476000	org/joda/time/chrono/GregorianChronology.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: C=86, ST=shanxi, L=xian, O=公司, OU=公司, CN=HF
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2022-07-25 10:57:56+00:00

Valid To: 2047-07-19 10:57:56+00:00
Issuer: C=86, ST=shanxi, L=xian, O=公司, OU=公司, CN=HF
Serial Number: 0x20d13bc0
Hash Algorithm: sha256
md5: 9ddbe193f88ebb7aeaf8195aec3a0b92
sha1: 1b5d871966e8f92e70d6c9f8eb54d49720ec252e
sha256: 0e32cf75e569427832661b461ddd9ebefe2575ac6a15a7117a192bf0cd914060
sha512: 98664c16cc9b7799959bc55d6295fe6e62987ae55857f501171fee9648961c1fc6191c3c32d6483e579af566e0752f1773570165a967084f2a5f9dc525452613
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 13fed7b26d95acbef6a3217f3f40ac386127fff38ad503f9ae6ac68259dedebd

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"
"target_scene_session" : "会话"

加壳分析

第三方SDK

名称	分类	URL链接
AutoNavi / Amap	Location	https://reports.exodus-privacy.eu.org/trackers/361

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.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.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.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.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
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
android.permission.ACCESS_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
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.CALL_PHONE	危险	直接拨打电话号码	允许应用程序在没有您干预的情况下拨打电话号码。恶意应用程序可能会导致您的电话账单出现意外呼叫。请注意,这不允许应用程序拨打紧急电话号码
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.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
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.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.sc.hxnf.ui.activity.SplashActivity	Schemes: alpverify://, Hosts: main,