MoGua

91官方 1.0.APK 分析报告

APP名称:	91官方

包名:	im.xyz.browserx
域名线索:	5条
URL线索:	4条
邮箱线索:	0条
分析日期:	2025年9月29日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: app0721.apk
文件大小: 1.54MB
MD5值: f787ef2f67330903e67ef6556e954984
SHA1值: 48b7ecf185be678af477a643d81c4953e9421d24
SHA256值: 31e6573bba1b0171f358d5b15f3845b6881b01f75b90fcb1a12156d12fee4318

APP 信息

App名称: 91官方
包名: im.xyz.browserx
主活动Activity: im.xyz.browserx.SplashActivity
安卓版本名称: 1.0
安卓版本: 1

域名线索

域名	服务器信息
schemas.android.com	没有服务器地理信息.
iwant.better2021life.com	**IP**: 104.21.78.241 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
m.baidu.com	**IP**: 110.242.68.10 **所属国家**: China **地区**: Hebei **城市**: Baoding **纬度**: 38.851109 **经度**: 115.490280
	IP: 104.21.54.50

we.killcovid2020.com	**所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.ebay.com	**IP**: 23.195.85.67 **所属国家**: Japan **地区**: Tokyo **城市**: Tokyo **纬度**: 35.689499 **经度**: 139.692322

URL线索

URL信息	Url所在文件
https://iwant.better2021life.com	c/a/a/i.java
https://www.ebay.com/usr/kellygolfjames	c/a/a/i.java
http://m.baidu.com/s?word=	c/a/a/e.java
http://schemas.android.com/apk/res/android	a/g/c/b/h.java
https://we.killcovid2020.com/index.php	im/xyz/browserx/MainActivity.java

邮箱线索

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=CA, ST=ON, L=London, O=Linksvalue media inc, OU=media, CN=James Chan
签名算法: rsassa_pkcs1v15
有效期自: 2021-01-21 16:30:37+00:00
有效期至: 2046-01-15 16:30:37+00:00
发行人: C=CA, ST=ON, L=London, O=Linksvalue media inc, OU=media, CN=James Chan
序列号: 0x1bef918d
哈希算法: sha256
md5值: f33786fef5cac0f04e090193fa28419a
sha1值: 97f51440a4e73b8642834a7d71f5c8adf78ff148
sha256值: 12dc7f1d71bbd8d3df598e6db43fe3f3c406adb01f8f66f96adde79419914d62
sha512值: 9c010a1509db59316305c531a1fe2712879a17f8fbda7593dfe5a3c809d09955481ce3fa11f4aaa7fc88dc00aa372dadbbcedd5e390b60a42f9b9a9779269792
公钥算法: rsa
密钥长度: 2048
指纹: c977513d99e2fe208fd7c52c11135928e0cd731ac5560266ec54bb2c9e808d04

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

应用内通信

活动(ACTIVITY)	通信(INTENT)
im.xyz.browserx.MainActivity	Schemes: https://, http://, file://, Mime Types: text/html, text/plain,

---