MoGua

Project slimBOXtv 1.7.APK 分析报告

APP名称: Project slimBOXtv

包名:	slim.box.tv.project
域名线索:	4条
URL线索:	1条
邮箱线索:	0条
分析日期:	2025年8月22日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: SBXproject_9.apk
文件大小: 0.38MB
MD5值: c3da535cb8c7ecd66fe43d07d9961ed7
SHA1值: 2bbb4348138224d80620f549ef8128500214b1b4
SHA256值: 6d1db535bf1695e4d0da7cc07fa3cfb1cb40e4c44f8b74405434599319e11810

APP 信息

App名称: Project slimBOXtv
包名: slim.box.tv.project
主活动Activity: slim.box.tv.project.MainActivity
安卓版本名称: 1.7
安卓版本: 5

域名线索

域名	服务器信息
slimboxtv.ru	**IP**: 46.30.40.108 **所属国家**: Netherlands **地区**: Noord-Holland **城市**: Amsterdam **纬度**: 52.378502 **经度**: 4.899980
qiwi.com	**IP**: 91.232.230.50 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752258 **经度**: 37.615471
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
yoomoney.ru	**IP**: 185.71.78.222 **所属国家**: Russian Federation **地区**: Moskva **城市**: Moscow **纬度**: 55.752258 **经度**: 37.615471

URL线索

URL信息	Url所在文件
https://t.me/mrSlimHouse	Mogua Engine V1
http://qiwi.com/n/SLIMBOX	Mogua Engine V1
https://yoomoney.ru/to/410012101149856	Mogua Engine V1
http://slimboxtv.ru	Mogua Engine V1
https://t.me/slimbox_chat	Mogua Engine V1

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: True
找到 1 个唯一证书
主题: C=RU, ST=slimBOXtv, L=krasnodar, O=slimBOXtv, OU=slimBOXtv, CN=slim, E=shbboxx@gmail.com
签名算法: rsassa_pkcs1v15
有效期自: 2021-10-28 21:18:06+00:00
有效期至: 2053-04-22 21:18:06+00:00
发行人: C=RU, ST=slimBOXtv, L=krasnodar, O=slimBOXtv, OU=slimBOXtv, CN=slim, E=shbboxx@gmail.com
序列号: 0xfb0e3489bac93ffa
哈希算法: sha1
md5值: acb38f8cdd553553743a9d199cde0c6b
sha1值: c06940b454fd9f909ddd9c25838d118d1daeb73b
sha256值: 414adf3f599b84ba52ef7f9e02e09363a9e421084683030389956be80d007df0
sha512值: 2f122912fa01c8176435a56c0297d49cac3a5ad4035e721be40f70bd154227a9ee5111071ac180e814725597bfe38937cfe6e7b99696e53f3902152d6e605b53
公钥算法: rsa
密钥长度: 1024
指纹: 8be8a6320be44fb238245a0b89ae6618109b8e22747c54f0d23ab20611ff40fd

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.ACCESS_SUPERUSER	未知	Unknown permission	Unknown permission from android reference
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_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.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.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.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.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.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.CHANGE_CONFIGURATION	系统需要	更改您的 UI 设置	允许应用程序更改当前配置,例如语言环境或整体字体大小
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.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.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.REAL_GET_TASKS	未知	Unknown permission	Unknown permission from android reference
android.permission.FORCE_STOP_PACKAGES	合法	强制停止其他应用程序	允许一个应用程序强行停止其他应用程序

应用内通信
