



东方赢家-机构版 1.0.APK 分析报告



APP名称:

东方赢家-机构版

包名:	ydrufg.bufrst.ycxrtezt
域名线索:	1条
URL线索:	1条
邮箱线索:	1条
分析日期:	2025年6月13日
分析平台:	摸瓜APK反编译平台

文件名: ydrufg.bufrst.ycxrtezt.apk
文件大小: 12.77MB
MD5值: 27927fb365027a375b0c4783a003815c
SHA1值: bfadce875b5b51d7a1e6aa668ac11d5f466840a1
SHA256值: 2e429dcf2335e2cbf29c9536e956268d71ab97c9c01b6d7b9e203af9b78ef881

i APP 信息

App名称: 东方赢家-机构版
包名: ydrufg.bufrst.ycxrtezt
主活动Activity: com.cacode.androidShell.HomeActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	服务器信息
kjur.github.io	IP: 185.199.109.153 所属国家: United States of America 地区: Pennsylvania 城市: California 纬度: 40.065647 经度: -79.891724

🌐 URL线索

URL信息	Url所在文件
https://kjur.github.io/jsrsasign/license/	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
kenji.urushima@gmail.com	摸瓜V2引擎

手机线索

签名证书

APK已签名
v1 签名: False
v2 签名: True
v3 签名: False
找到 1 个唯一证书
主题: C=ugdcifqkxzvdj, ST=ywbwliwqnxsm, L=oyeumjyhxeihr, O=nem1740965177732, OU=lro1740965177732, CN=TG@apken888
签名算法: rsassa_pkcs1v15
有效期自: 2025-03-03 01:26:17+00:00
有效期至: 2075-02-19 01:26:17+00:00
发行人: C=ugdcifqkxzvdj, ST=ywbwliwqnxsm, L=oyeumjyhxeihr, O=nem1740965177732, OU=lro1740965177732, CN=TG@apken888
序列号: 0x22415a61
哈希算法: sha1
md5值: c3d12a6a341405d11eef0dec025d11be
sha1值: 3700d395624913f7d3daf339a108f67c1390639b
sha256值: fc6e052e57e5694a1368ce6f78475ab7f0dc1cb8bb30b124d5bdd17e8978d9c0
sha512值: c81090eeff8a75c1470a3e4bf4b30fe61b8c255719b27ae603e436b06a721d8f0c81215cb6d90d90e4f665ac2a0181dc1971bdd3b8e8b9b2639a76510a353235
公钥算法: rsa
密钥长度: 1024
指纹: 9067410bbaa6950e158389b112028dc10040bbcb7688d60568d76661c3eaa9a8

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