



MoGua

东方证券 1.1.0.APK 分析报告



东方证券
ORIENT SECURITIES

APP名称:

东方证券

包名:	flymfo.oncayl.zywwzcrye
域名线索:	5条
URL线索:	4条
邮箱线索:	1条
分析日期:	2024年10月30日
分析平台:	摸瓜APK反编译平台

文件名: 4c11cb.apk

文件大小: 60.44MB

MD5值: 2bb1eaf4cb41e37b31776b90294c11cb

SHA1值: 1d4540f22577d74d9473cb3721d87d4b806fc809

SHA256值: df11536e98305e237b2bd34a9b4e3d8eaea943cd3749c622ad91ff12eb1dc351

i APP 信息

App名称: 东方证券

包名: flymfo.oncayl.zywwzcrye

主活动Activity: com.max.securities.dongfang.MainActivity

安卓版本名称: 1.1.0

安卓版本: 11

🔍 域名线索

域名	服务器信息
www.w3.org	IP: 104.18.22.19 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
element.eleme.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
mths.be	IP: 83.137.145.144 所属国家: Netherlands 地区: Groningen

	城市: Groningen 纬度: 53.219173 经度: 6.567002
npms.io	IP: 104.21.49.221 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
feross.org	IP: 50.116.11.184 所属国家: United States of America 地区: California 城市: Fremont 纬度: 37.548271 经度: -121.988571

URL线索

URL信息	Url所在文件
https://npms.io/search?q=ponyfill	摸瓜V2引擎
http://element.eleme.io/	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d	摸瓜V2引擎
http://feross.org >	摸瓜V2引擎
https://mths.be/punycode	摸瓜V2引擎
http://a	摸瓜V2引擎

http://a	摸瓜V2引擎
http://a/c%20d	摸瓜V2引擎
https://feross.org/opensource>	摸瓜V2引擎
http://feross.org>	摸瓜V2引擎
https://mths.be/punycode	摸瓜V2引擎
http://a	摸瓜V2引擎
http://a/c%20d	摸瓜V2引擎
https://feross.org/opensource>	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
jintongxue2018@163.com	摸瓜V2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=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

签名算法: rsassa_pkcs1v15

有效期自: 2024-03-26 13:28:04+00:00

有效期至: 2078-12-28 13:28:04+00:00

发行人: C=Unknown, ST=Unknown, L=Unknown, O=Unknown, OU=Unknown, CN=Unknown

序列号: 0x7dc908bf

哈希算法: sha256

md5值: b6a0831090ca7b16d208fc391642cd46

sha1值: 607f2b54528d544edc792798c227d6ef791fb6ef

sha256值: 989e17e8b08a64b6d0ebc9459f5ea741081a65dcd9f65301315047e48da44ab6

sha512值: 7f735954add6cc99d7a88897a40b5bfa62d1373a6db53f45d2ac5c99268583981581717642a9723c1c069856b8768ea8253f72145b9610f14bb9c0f02883a672

公钥算法: rsa

密钥长度: 2048

指纹: fe6e2f466d2545f37e9b30532e5f2a54742d8d91ed997d00973801f946656146

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
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.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_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
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

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。