MoGua

科技强国 1.7.8.APK 分析报告

APP名称: 科技强国

包名:	uni.UNI1EFA605
域名线索:	34条
URL线索:	8条
邮箱线索:	2条
分析日期:	2025年6月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 科技强国.apk
文件大小: 19.51MB
MD5值: c6936ac348ebd9dfd1ea9c40e4ebe6d5
SHA1值: 3ff4ede988739235aeea591538d41e822757cda2
SHA256值: 90b1cf099b47b8be51f74a4b2f89109209bf35fda5b3652501aa3b8a370f033c

APP 信息

App名称: 科技强国
包名: uni.UNI1EFA605
主活动Activity: io.dcloud.PandoraEntry
安卓版本名称: 1.7.8
安卓版本: 178

域名线索

域名	服务器信息
tronscan.org	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
uniapp.dcloud.net.cn	**IP**: 123.125.244.28 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
	IP: 172.66.43.93 **所属国家**: United States of America **地区**: California

quilljs.com	**城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.ilovememo.com	**IP**: 116.130.221.21 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.apache.org	**IP**: 151.101.2.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.google.com	**IP**: 31.13.73.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
service.dcloud.net.cn	**IP**: 111.229.199.57 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
cdn-technology.com	**IP**: 199.91.74.171 **所属国家**: Mexico **地区**: Ciudad de Mexico **城市**: Mexico City **纬度**: 19.428471 **经度**: -99.127609

sun.io	**IP**: 104.18.3.230 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.bspapp.com	**IP**: 39.96.249.142 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
mashengke.com	**IP**: 163.142.153.213 **所属国家**: China **地区**: Guangdong **城市**: Foshan **纬度**: 23.026770 **经度**: 113.131477
www.ccbtc.org.cn	**IP**: 121.29.37.164 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
www.okx.com	**IP**: 169.254.0.2 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
www.binance.com	**IP**: 0.0.0.0 **所属国家**: - **地区**: - **城市**: -

	纬度: 0.000000 **经度**: 0.000000
html2canvas.hertzen.com	IP: 104.21.65.51 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
cdn-technology.net	IP: 199.91.74.171 **所属国家**: Mexico **地区**: Ciudad de Mexico **城市**: Mexico City **纬度**: 19.428471 **经度**: -99.127609
www.cas.cn	IP: 159.226.242.61 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api-kejicn.net	IP: 154.198.227.74 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
www.w3.org	IP: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 20.205.243.166 **所属国家**: Singapore

github.com	**地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
tron.network	IP: 203.111.254.117 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
api.168baby.com	IP: 116.130.221.21 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
occupationexam.com	没有服务器地理信息.
tongji.dcloud.io	IP: 115.159.211.231 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api.next.bspapp.com	IP: 203.107.60.33 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
apis.map.qq.com	IP: 116.130.224.140 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501

	经度: 116.397102
ask.dcloud.net.cn	**IP**: 123.125.244.31 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
www.xuexi.cn	**IP**: 211.154.222.119 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
api-kejicn.com	**IP**: 154.198.227.49 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052570 **经度**: -118.243904
vkceyugu.cdn.bspapp.com	**IP**: 124.95.153.241 **所属国家**: China **地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
www.tronlink.org	**IP**: 208.101.60.87 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.339390 **经度**: -121.894958
	IP: 104.21.87.173 **所属国家**: United States of America

ave.ai	**地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.gov.cn	**IP**: 113.5.65.14 **所属国家**: China **地区**: Heilongjiang **城市**: Harbin **纬度**: 45.750000 **经度**: 126.650002
hertzen.com	**IP**: 172.67.140.170 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL信息	Url所在文件
https://ask.dcloud.net.cn/article/36199	摸瓜V1引擎
https://apis.map.qq.com/jsapi?qt=translate&type=1&points=	摸瓜V2引擎
https://apis.map.qq.com/uri/v1/routeplan?type=drive&to=	摸瓜V2引擎
https://www.google.com/maps/?daddr=	摸瓜V2引擎
https://www.google.com/maps/	摸瓜V2引擎
https://quillis.com/	摸瓜V2引擎

https://quilljs.com/	摸瓜V2引擎
https://quilljs.com	摸瓜V2引擎
https://api-kejicn.com	摸瓜V2引擎
https://api-kejicn.net	摸瓜V2引擎
https://cdn-technology.net	摸瓜V2引擎
https://cdn-technology.com	摸瓜V2引擎
https://api.168baby.com	摸瓜V2引擎
https://api.ilovememo.com	摸瓜V2引擎
https://tongji.dcloud.io/uni/stat	摸瓜V2引擎
https://tongji.dcloud.io/uni/stat.gif?	摸瓜V2引擎
https://github.com/emn178/js-md5	摸瓜V2引擎
https://www.gov.cn	摸瓜V2引擎
https://www.xuexi.cn	摸瓜V2引擎
https://www.cas.cn	摸瓜V2引擎
https://www.ccbtc.org.cn/jinzhuan/index_pc.html	摸瓜V2引擎
https://tronscan.org/	摸瓜V2引擎
https://www.okx.com/zh-hans/web3	摸瓜V2引擎
https://www.binance.com/zh-CN/web3wallet	摸瓜V2引擎

https://ave.ai	摸瓜V2引擎
https://sun.io/	摸瓜V2引擎
https://tron.network/index?lng=zh	摸瓜V2引擎
https://www.tronlink.org/cn/	摸瓜V2引擎
https://api.next.bspapp.com	摸瓜V2引擎
https://api.bspapp.com	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/secure-network.html	摸瓜V2引擎
https://uniapp.dcloud.net.cn/uniCloud/faq?id=promise	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://vkceyugu.cdn.bspapp.com/VKCEYUGU-6bef1fe3-e3e3-4909-9f0c-6ed9bd11c93b/aae2360a-6628-4c93-b873-ce1600b9a852.apk	摸瓜V2引擎
https://occupationexam.com	摸瓜V2引擎
https://mashengke.com/home-video/ys-300.png	摸瓜V2引擎
https://html2canvas.hertzen.com>	摸瓜V2引擎
https://hertzen.com>	摸瓜V2引擎
https://github.com/facebook/regenerator/blob/main/LICENSE	摸瓜V2引擎
https://service.dcloud.net.cn/uniapp/feedback.html	摸瓜V2引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V2引擎
https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎

https://github.com/ecomfe/zrender/blob/master/LICENSE.txt	摸瓜V2引擎

邮箱线索

邮箱地址	所在文件
emn178@gmail.com jhruby.web@gmail.com	摸瓜V2引擎
jhruby.web@gmail.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=cn, ST=bj, L=bj, O=beijing, OU=beijing, CN=zs
签名算法: rsassa_pkcs1v15
有效期自: 2024-08-31 15:25:44+00:00
有效期至: 2124-08-07 15:25:44+00:00
发行人: C=cn, ST=bj, L=bj, O=beijing, OU=beijing, CN=zs
序列号: 0xb46647b
哈希算法: sha256
md5值: 6acdd6a77d3067452b9e32f1e0339314
sha1值: fce53789ba28bd3d0dad15bbcc489a861f5008f1
sha256值: ec86e6190c99dd23da92c5b34af11ddc75318fee348742fc3ecfb62ef5e2b0a4
sha512值: e64dc73d98a0004b3fd97ee8b03474dae0c8314a25a1a31db1bc6150fbb63a6eeb042a65e3cf85cc7c53a744e7c3e2803a60d9a46183169e065aa2a363cb850e
公钥算法: rsa
密钥长度: 2048

指纹: 26b1543655b12dbe0e008d747c56c2873a27f22f27cfc9b75898d9beba4a7092

硬编码敏感信息

可能的敏感信息
"dcloud_common_user_refuse_api" : "the user denies access to the API"
"dcloud_io_without_authorization" : "not authorized"
"dcloud_oauth_authentication_failed" : "failed to obtain authorization to log in to the authentication service"
"dcloud_oauth_empower_failed" : "the Authentication Service operation to obtain authorized logon failed"
"dcloud_oauth_logout_tips" : "not logged in or logged out"
"dcloud_oauth_oauth_not_empower" : "oAuth authorization has not been obtained"
"dcloud_oauth_token_failed" : "failed to get token"
"dcloud_permissions_reauthorization" : "reauthorize"
"dcloud_tips_certificate" : "certificate"
"dcloud_common_user_refuse_api" : "用户拒绝该API访问"
"dcloud_io_without_authorization" : "没有获得授权"
"dcloud_oauth_authentication_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_empower_failed" : "获取授权登录认证服务操作失败"
"dcloud_oauth_logout_tips" : "未登录或登录已注销"

"dcloud_oauth_oauth_not_empower" : "尚未获取oauth授权"
"dcloud_oauth_token_failed" : "获取token失败"
"dcloud_permissions_reauthorization" : "重新授权"
"dcloud_tips_certificate" : "证书"

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**	**类型**	**详细情况**

	险		
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.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_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.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.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
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
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
android.permission.GET_ACCOUNTS	危险	列出帐户	允许访问账户服务中的账户列表
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.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.FLASHLIGHT	正常	控制手电筒	允许应用程序控制手电筒
android.permission.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
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.QUERY_ALL_PACKAGES	正常		允许查询设备上的任何普通应用程序,无论清单声明如何
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
getui.permission.GetuiService.uni.UNI1EFA605	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_IMAGES	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VIDEO	未知	Unknown permission	Unknown permission from android reference
android.permission.READ_MEDIA_VISUAL_USER_SELECTED	未知	Unknown permission	Unknown permission from android reference
com.huawei.android.launcher.permission.CHANGE_BADGE	正常	在应用程序上显示通知计数	在华为手机的应用程序启动图标上显示通知计数或徽章。
com.vivo.notification.permission.BADGE_ICON	未知	Unknown permission	Unknown permission from android reference
com.asus.msa.SupplementaryDID.ACCESS	未知	Unknown permission	Unknown permission from android reference
android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作

android.permission.SCHEDULE_EXACT_ALARM	正常		允许应用程序使用精确的警报调度 API 来执行对时敏感的后台工作
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_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_BACKGROUND_LOCATION	危险	后台访问位置	允许应用程序在后台访问位置
freemme.permission.msa	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
io.dcloud.PandoraEntry	Schemes: unipush://, hbuilder://, kjqg://, Hosts: io.dcloud.unipush, Paths: /,