MoGua

优途加速器 1.2.43.APK 分析报告

APP名称:	优途加速器

包名:	com.lzz.youtu
域名线索:	14条
URL线索:	22条
邮箱线索:	1条
分析日期:	2025年7月16日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 优途加速器.apk

文件大小: 10.16MB
MD5值: 50f77368904bbdad254499c6da1323c6
SHA1值: d0b2f735eebe527f62b4aa69f1e0a1ce5009db08
SHA256值: 7b04b2c3a36a7e090166808fcf3e8f320ad844cacb2c5657ded727aa36ac3555

APP 信息

App名称: 优途加速器
包名: com.lzz.youtu
主活动Activity: com.lzz.youtu.ui.OpenActivity
安卓版本名称: 1.2.43
安卓版本: 106

域名线索

域名	服务器信息
www.alibaba.com	**IP**: 203.119.238.64 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
url.cn	**IP**: 60.29.239.156 **所属国家**: China **地区**: Tianjin **城市**: Tianjin **纬度**: 39.142181 **经度**: 117.176102
www.google.com	**IP**: 31.13.68.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin

	纬度: 53.344151 **经度**: -6.267249
crashpad.chromium.org	IP: 142.250.73.83 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
192.168.0.104	IP: 192.168.0.104 **所属国家**: - **地区**: - **城市**: - **纬度**: 0.000000 **经度**: 0.000000
wallpapercave.com	IP: 104.22.53.71 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
you-tu-99f54.firebaseio.com	IP: 35.190.39.113 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
netty.io	IP: 104.21.3.132 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 34.49.79.89

www.openssl.org	**所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.eclipse.org	**IP**: 198.41.30.198 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347 **经度**: -79.711548
tools.ietf.org	**IP**: 104.16.45.99 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.youtuvpn.com	**IP**: 165.154.110.172 **所属国家**: Hong Kong **地区**: Hong Kong **城市**: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
github.com	**IP**: 20.205.243.166 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
wiki.eclipse.org	**IP**: 198.41.30.195 **所属国家**: Canada **地区**: Ontario **城市**: Brampton **纬度**: 43.702347

	经度: -79.711548

URL线索

URL信息	Url所在文件
https://url.cn/ce420a23?_type=wpa&qidian=true\	com/lzz/youtu/App.java
http://%s:%s@%s	com/lzz/youtu/ss/tunnel/httpconnect/HttpConnectConfig.java
http://www.youtuvpn.com	com/lzz/youtu/network/LocalDataManager.java
https://www.google.com	com/lzz/youtu/pojo/UserInfo.java
https://wallpapercave.com/wp/wp5893437.jpg	com/lzz/youtu/pojo/UserInfo.java
https://www.alibaba.com/index.html	com/lzz/youtu/ui/WebActivity.java
http://192.168.0.104:8080/	com/lzz/youtu/ui/WebActivity.java
https://tools.ietf.org/html/rfc7540	io/netty/handler/codec/http2/HttpConversionUtil.java
https://wiki.eclipse.org/Jetty/Feature/NPN	io/netty/handler/ssl/JdkNpnApplicationProtocolNegotiator.java
https://netty.io/wiki/forked-tomcat-native.html	io/netty/handler/ssl/OpenSsl.java
https://www.openssl.org/docs/man1.0.2/apps/verify.html.	io/netty/handler/ssl/OpenSslCertificateException.java
http://www.eclipse.org/jetty/documentation/current/alpn-chapter.html	io/netty/handler/ssl/JdkAlpnApplicationProtocolNegotiator.java
https://netty.io/wiki/sslcontextbuilder-and-private-key.html	io/netty/handler/ssl/PemReader.java

https://netty.io/wiki/reference-counted-objects.html	io/netty/util/ResourceLeakDetector.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Completable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Single.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Maybe.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Observable.java
https://github.com/ReactiveX/RxJava/wiki/Plugins	io/reactivex/Flowable.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	io/reactivex/exceptions/OnErrorNotImplementedException.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	io/reactivex/exceptions/UndeliverableException.java
https://you-tu-99f54.firebaseio.com	摸瓜V1引擎
https://crashpad.chromium.org/bug/new	lib/arm64-v8a/libcrashlytics-common.so
https://crashpad.chromium.org/	lib/arm64-v8a/libcrashlytics-common.so

邮箱线索

邮箱地址	所在文件
yuuttojsq@gmail.com	摸瓜V1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: False
找到 1 个唯一证书
主题: C=China, L=CN, O=ApkSigner, CN=ApkSigner
签名算法: rsassa_pkcs1v15
有效期自: 3870-01-31 17:01:01+00:00
有效期至: 2900-02-04 17:01:01+00:00
发行人: C=China, L=CN, O=ApkSigner, CN=ApkSigner
序列号: 0x1315d520
哈希算法: sha256
md5值: 8a92fadaf140fdc9e73939fd3d9ccc91
sha1值: e6067b97bea6720899676d717f9a39a38749ea2b
sha256值: 291dba8f8082e25c25a2024bf2f91252335361904 78ebe0e44a676b0b1ba1694
sha512值: c88290350af3c1b07bf398d51ab4a358ad11e5eece3d4c15ec375bef7c4bcd4a0b5ce9a227213762affad439ba2ea5099c2882f85a71301444a64f27052d3028
公钥算法: rsa
密钥长度: 2048
指纹: a9aa080f201c3df4071a988ce147ec17bf8018d696da9aebb562101e8d8991b7

硬编码敏感信息

可能的敏感信息
"firebase_database_url" : "https://you-tu-99f54.firebaseio.com"
"google_api_key" : "AIzaSyDqTc26lpcMqaRq19vzVklnUEzASnvjEO8"
"google_crash_reporting_api_key" : "AIzaSyDqTc26lpcMqaRq19vzVklnUEzASnvjEO8"
"resource_common_pwd" : "密码"
"resource_common_src_pwd" : "原密码"

"resource_common_user" : "账号"
"resource_common_username" : "用户名"
"resource_user_login_user" : "登录账号 >"
"toast_user_input_password" : "请先输入您的密码"
"toast_user_input_user" : "请输入您的用户名"
"toast_vpn_session_invalid" : "session无效,请重新登录."
"resource_common_pwd" : "Password"
"resource_common_src_pwd" : "Original password"
"resource_common_user" : "Account"
"resource_common_username" : "Username"
"resource_user_login_user" : "Login account >"
"toast_user_input_password" : "Please enter your password"
"toast_user_input_user" : "Please enter your username"
"toast_vpn_session_invalid" : "session invalid, please log in again."

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.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.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_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.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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.REQUEST_IGNORE_BATTERY_OPTIMIZATIONS	正常		应用程序必须持有的权限才能使用 Settings.ACTION_REQUEST_IGNORE_BATTERY_OPTIMIZATIONS。
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.tencent.tauth.AuthActivity	Schemes: tencent1106779540://,