MoGua

Touro box1 1.1.0.APK 分析报告

APP名称: Touro box1

包名:	com.new2tourosat.app
域名线索:	18条
URL线索:	31条
邮箱线索:	1条
分析日期:	2025年1月30日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Tourobox1.apk
文件大小: 11.26MB
MD5值: d0ea4f82c067dfabc3cf14bbceaf6d8c
SHA1值: e2b40b4faf0306e517e76a88211726e1a7d5ca4d
SHA256值: d046b73d4534c52b3913fa308991f5bffdc418fd82aa313a49aba26249072ca4

APP 信息

App名称: Touro box1
包名: com.new2tourosat.app
主活动Activity: com.newott.app.ui.auth.active.AuthActiveActivity
安卓版本名称: 1.1.0
安卓版本: 15

域名线索

域名	服务器信息
pagead2.googlesyndication.com	**IP**: 203.208.50.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
firebase-settings.crashlytics.com	**IP**: 220.181.174.226 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
developer.apple.com	**IP**: 17.253.87.206 **所属国家**: Hong Kong **地区**: Hong Kong

	城市: Hong Kong **纬度**: 22.285521 **经度**: 114.157692
exoplayer.dev	IP: 185.199.109.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708
update.crashlytics.com	IP: 203.208.50.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
www.google.com	IP: 128.242.240.91 **所属国家**: United States of America **地区**: California **城市**: Milpitas **纬度**: 37.428268 **经度**: -121.906616
reports.crashlytics.com	没有服务器地理信息.
www.w3.org	IP: 128.30.52.100 **所属国家**: United States of America **地区**: Massachusetts **城市**: Cambridge **纬度**: 42.365078 **经度**: -71.104523
google.com	IP: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464272 **经度**: 9.189510

www.googleadservices.com	**IP**: 203.208.50.166 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
goo.gl	**IP**: 142.251.42.238 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
schemas.android.com	没有服务器地理信息.
play.google.com	**IP**: 172.217.160.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
app-measurement.com	**IP**: 220.181.174.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397232
activecode.turoisherego.xyz	**IP**: 104.21.12.7 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
	IP: 54.89.135.129

plus.google.com	**所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.043720 **经度**: -77.487488
firebase.google.com	IP: 172.217.160.78 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
aomedia.org	IP: 185.199.108.153 **所属国家**: United States of America **地区**: Pennsylvania **城市**: California **纬度**: 40.065632 **经度**: -79.891708

URL线索

URL信息	Url所在文件
http://schemas.android.com/apk/res/android	d/h/d/b/h.java
https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	f/d/c/l/b.java
https://update.crashlytics.com/spi/v1/platforms/android/apps	f/d/c/l/f/m/h.java
https://update.crashlytics.com/spi/v1/platforms/android/apps/%s	f/d/c/l/f/m/h.java
https://reports.crashlytics.com/spi/v1/platforms/android/apps/%s/reports	f/d/c/l/f/m/h.java
https://reports.crashlytics.com/sdk-api/v1/platforms/android/apps/%s/minidumps	f/d/c/l/f/m/h.java

https://firebase.google.com/support/privacy/init-options.	f/d/c/r/d.java
https://app-measurement.com/a	f/d/a/c/i/f/t8.java
https://goo.gl/J1sWQy	f/d/a/c/i/f/e0.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	f/d/a/c/a/a/b.java
https://app-measurement.com/a	f/d/a/c/j/b/x2.java
https://www.google.com	f/d/a/c/j/b/l6.java
https://google.com/search?	f/d/a/c/j/b/k6.java
https://firebase.google.com/support/guides/disable-analytics	f/d/a/c/j/b/c3.java
https://goo.gl/NAOOOI.	f/d/a/c/j/b/k9.java
https://goo.gl/NAOOOI	f/d/a/c/j/b/k9.java
https://www.googleadservices.com/pagead/conversion/app/deeplink? id_type=adid&sdk_version=%s&rdid=%s&bundleid=%s&retry=%s	f/d/a/c/j/b/o5.java
https://plus.google.com/	f/d/a/c/e/o/o0.java
https://exoplayer.dev/issues/player-accessed-on-wrong-thread	f/d/a/b/v0.java
http://www.w3.org/ns/ttml	f/d/a/b/i1/r/a.java
https://aomedia.org/emsg/ID3	f/d/a/b/g1/h/a.java
https://developer.apple.com/streaming/emsg-id3	f/d/a/b/g1/h/a.java
https://activecode.turoisherego.xyz/touro/setsetting.php?	f/i/a/l/m.java

https://activecode.turoisherego.xyz/touro/youtubetrailer.php?	f/i/a/l/j.java
https://activecode.turoisherego.xyz/touro/getfav.php?	f/i/a/l/k.java
https://activecode.turoisherego.xyz/touro/setfav.php?	f/i/a/l/k.java
https://activecode.turoisherego.xyz/touro/parseresetgo.php	f/i/a/l/e.java
https://activecode.turoisherego.xyz/touro/setfav.php?	f/i/a/l/b0.java
https://activecode.turoisherego.xyz/touro/checkifuid.php?	f/i/a/l/b.java
https://activecode.turoisherego.xyz/touro/activecode.php	f/i/a/l/c.java
https://activecode.turoisherego.xyz/touro/activecode.php	f/i/a/l/d.java
https://www.google.com/	f/i/a/i/a/a/a.java
https://www.google.com/	f/i/a/j/a/b.java
https://play.google.com/store/apps/details?id=	f/i/a/m/f/f/f.java
https://activecode.turoisherego.xyz/touro/activecode.php	com/newott/app/data/model/favorite/FavoriteItem.java
https://play.google.com/store/apps/details?id=	com/newott/app/ui/newSettings/SettingsDialog.java

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	f/d/a/c/e/c0.java

手机线索

手机号	所在文件
15552000000	f/d/a/c/j/b/m6.java
15222222222	f/d/a/b/e1/a0/d.java

签名证书

APK is signed
v1 signature: True
v2 signature: True
v3 signature: False
Found 1 unique certificates
Subject: CN=SpiderKeyStore2
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2020-11-10 12:37:05+00:00
Valid To: 2045-11-04 12:37:05+00:00
Issuer: CN=SpiderKeyStore2
Serial Number: 0x39f0a8c7
Hash Algorithm: sha256
md5: fb440e0b0b3e1f2ab0fa525772518ee9
sha1: 427ce3344b32d2c179eb57a5a55464eb56331dc4
sha256: 8f999289f3ee6472ffcf1051390afcdf5432ea071f8817346a7722177fae9fde
sha512: be5faf706a352c0d79542d621ec95eee7561dcb5e49b412284987654c0adf15dd8580000c95a68d4c7a9c209ee3be0229cec8e39795775625f8bc394c338d417
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: 8c4a657d846bf814c01ee031a0bf88085d8181fc0d4c40d1b689bcd15629b7fa

硬编码敏感信息

可能的敏感信息
"google_api_key" : "AIzaSyC_tryLykG3Y8Ktey-8740N1qKCwXCPysk"
"google_crash_reporting_api_key" : "AIzaSyC_tryLykG3Y8Ktey-8740N1qKCwXCPysk"
"password" : "Password"
"username" : "UserName"
"write_password" : "please write password"
"wrong_password" : "wrong password"
"password" : "Senha"
"username" : "Usuario"
"write_password" : "por favor escreva a senha"
"wrong_password" : "senha incorreta"

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_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.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.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.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.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.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
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	未知	Unknown permission	Unknown permission from android reference

应用内通信
