MoGua

GalaxyVPN 2.1.5.APK 分析报告

APP名称: GalaxyVPN

包名:	com.galaxylab.ss
域名线索:	38条
URL线索:	28条
邮箱线索:	0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: 银河VPN.apk
文件大小: 33.74MB
MD5值: 5e7ba9cc75afafd94f0d8cff4b2a785d
SHA1值: 59a3abdc44d813feb756c767de4d3e00955ba395
SHA256值: e89703950342adf966e72501481644a0235e9d678bcf8bf1d6c7dc16645cf255

APP 信息

App名称: GalaxyVPN
包名: com.galaxylab.ss
主活动Activity: com.galaxylab.android.SplashActivity
安卓版本名称: 2.1.5
安卓版本: 115

域名线索

域名	服务器信息
api.msmaster.qa.paypal.com	没有服务器地理信息.
app-measurement.com	**IP**: 114.250.64.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
checkout.paypal.com	**IP**: 172.64.153.163 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

api.paypal.com	**IP**: 64.4.249.23 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
c.sandbox.paypal.com	**IP**: 151.101.91.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
mobile.events.data.microsoft.com	**IP**: 13.89.178.27 **所属国家**: United States of America **地区**: Iowa **城市**: Des Moines **纬度**: 41.600449 **经度**: -93.609116
in1-gw2-01-ce7dd027.eastus2.cloudapp.azure.com	没有服务器地理信息.
www.facebook.com	**IP**: 31.13.73.9 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
api-m.sandbox.paypal.com	**IP**: 151.101.91.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
outcome-arm-ext-med-ext.sonic-us.supersonicads.com	没有服务器地理信息.

c.paypal.com	IP: 151.101.89.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.paypalobjects.com	IP: 151.101.91.1 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api-m.paypal.com	IP: 104.16.123.74 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
graph.facebook.com	IP: 104.244.43.182 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
goo.gl	IP: 142.250.69.174 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
api.sandbox.braintreegateway.com	IP: 159.242.242.128 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.385639

	经度: -121.885277
in.appcenter.ms	**IP**: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547
uri.paypal.com	没有服务器地理信息.
outcome-ssp.supersonicads.com	**IP**: 3.169.231.65 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.627499 **经度**: -122.346199
api.braintreegateway.com	**IP**: 35.156.167.229 **所属国家**: Germany **地区**: Hessen **城市**: Frankfurt am Main **纬度**: 50.110882 **经度**: 8.681996
developers.braintreepayments.com	**IP**: 151.101.89.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.apkgalaxylab.com	**IP**: 35.155.85.218 **所属国家**: United States of America **地区**: Oregon **城市**: Boardman **纬度**: 45.839859 **经度**: -119.700577

api.sandbox.paypal.com	**IP**: 173.0.93.228 **所属国家**: United States of America **地区**: California **城市**: San Jose **纬度**: 37.385639 **经度**: -121.885277
backup2.apkgalaxylab.com	没有服务器地理信息.
outcome-crash-report.supersonicads.com	没有服务器地理信息.
b.stats.paypal.com	**IP**: 34.147.177.40 **所属国家**: United Kingdom of Great Britain and Northern Ireland **地区**: England **城市**: London **纬度**: 51.508530 **经度**: -0.125740
in2-prod-east-us2-23fa330.trafficmanager.net	**IP**: 4.152.45.235 **所属国家**: United States of America **地区**: Virginia **城市**: Boydton **纬度**: 36.667641 **经度**: -78.387497
www.slf4j.org	**IP**: 195.15.222.169 **所属国家**: Switzerland **地区**: Geneve **城市**: Carouge **纬度**: 46.180931 **经度**: 6.138709
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

star.c10r.facebook.com	**IP**: 202.160.129.37 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
shadowsocks.org	**IP**: 8.7.198.45 **所属国家**: United States of America **地区**: Louisiana **城市**: Monroe **纬度**: 32.548328 **经度**: -92.045235
assets.staging.braintreepayments.com	没有服务器地理信息.
init.supersonicads.com	**IP**: 18.155.202.2 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
star-mini.c10r.facebook.com	**IP**: 103.252.114.61 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
api.facebook.com	**IP**: 202.160.129.37 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
	IP: 10.0.2.2 **所属国家**: - **地区**: -

10.0.2.2	**城市**: - **纬度**: 0.000000 **经度**: 0.000000
galaxylab2019-b0baa.firebaseio.com	**IP**: 35.201.97.85 **所属国家**: United States of America **地区**: Missouri **城市**: Kansas City **纬度**: 39.099731 **经度**: -94.578568
scontent-iad3-2.xx.fbcdn.net	**IP**: 157.240.229.1 **所属国家**: United States of America **地区**: Virginia **城市**: Dulles **纬度**: 38.951668 **经度**: -77.448059

URL线索

URL**信息**	Url**所在文件**
https://developers.braintreepayments.com/guides/client-sdk/android/v2	com/braintreepayments/api/n.java
https://developers.braintreepayments.com/guides/paypal/overview/android/	com/braintreepayments/api/i.java
https://developers.braintreepayments.com/guides/client-sdk/android/	com/braintreepayments/api/i.java
http://10.0.2.2:3000/	com/braintreepayments/api/v/p0.java
https://api.sandbox.braintreegateway.com/	com/braintreepayments/api/v/p0.java
https://api.braintreegateway.com/	com/braintreepayments/api/v/p0.java

https://api.paypal.com	com/braintreepayments/api/v/a0.java
https://api.sandbox.paypal.com	com/braintreepayments/api/v/a0.java
https://api.msmaster.qa.paypal.com	com/braintreepayments/api/v/a0.java
https://api.sandbox.braintreegateway.com:443/merchants/	com/braintreepayments/api/v/a0.java
https://api.braintreegateway.com:443/merchants/	com/braintreepayments/api/v/a0.java
https://github.com/braintree/browser-switch-android	com/braintreepayments/browserswitch/b.java
https://shadowsocks.org/acl/android/v1/	com/github/shadowsocks/acl/AclSyncer.java
http://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData	com/ironsource/mediationsdk/u1/a.java
http://outcome-arm-ext-med-ext.sonic-us.supersonicads.com/aemData	com/ironsource/mediationsdk/u1/o.java
https://outcome-ssp.supersonicads.com/mediation?adUnit=3	com/ironsource/mediationsdk/k1/f.java
https://outcome-ssp.supersonicads.com/mediation?adUnit=2	com/ironsource/mediationsdk/k1/e.java
https://init.supersonicads.com/sdk/v	com/ironsource/mediationsdk/r1/b.java
https://outcome-crash-report.supersonicads.com/reporter	com/ironsource/environment/f.java
https://app-measurement.com/a	e/g/b/c/f/j/rb.java
https://goo.gl/J1sWQy	e/g/b/c/f/j/g.java
https://in.appcenter.ms	e/j/a/m/a.java
https://mobile.events.data.microsoft.com/OneCollector/1.0	e/j/a/m/c.java
https://api-m.paypal.com/v1/	e/k/a/a/b/a/d.java

https://api-m.paypal.com/v1/	e/k/a/a/b/a/l/a.java
https://api-m.sandbox.paypal.com/v1/	e/k/a/a/b/a/l/a.java
https://uri.paypal.com/services/payments/futurepayments\	e/k/a/a/b/a/h/e.java
https://checkout.paypal.com/one-touch-login/\	e/k/a/a/b/a/h/e.java
https://assets.staging.braintreepayments.com/one-touch-login/\	e/k/a/a/b/a/h/e.java
https://www.paypalobjects.com/webstatic/otc/otc-config.android.json	e/k/a/a/b/a/h/e.java
https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes_config_android_v4.json	h/a/a/a/a/k.java
https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes_android_rc_v1.json	h/a/a/a/a/m/m.java
https://c.paypal.com/r/v1/device/client-metadata	h/a/a/a/a/m/o.java
https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes_config_android_v4.json	h/a/a/a/a/m/o.java
https://www.paypalobjects.com/digitalassets/c/rda-magnes/magnes_config_android_v4.json	h/a/a/a/a/m/p.java
https://b.stats.paypal.com/counter.cgi	h/a/a/a/a/m/c.java
https://c.sandbox.paypal.com/r/v1/device/client-metadata	h/a/a/a/a/m/d.java
https://c.paypal.com/r/v1/device/client-metadata	h/a/a/a/a/m/d.java
http://www.slf4j.org/codes.html	l/b/c.java
https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.md	摸瓜V1引擎
https://galaxylab2019-b0baa.firebaseio.com	摸瓜V1引擎

https://github.com/shadowsocks/shadowsocks-android/blob/master/.github/faq.ru.md	摸瓜V1引擎
api.facebook.com	摸瓜V3引擎
graph.facebook.com	摸瓜V3引擎
in1-gw2-01-ce7dd027.eastus2.cloudapp.azure.com	摸瓜V3引擎
backup2.apkgalaxylab.com	摸瓜V3引擎
in.appcenter.ms	摸瓜V3引擎
scontent-iad3-2.xx.fbcdn.net	摸瓜V3引擎
in2-prod-east-us2-23fa330.trafficmanager.net	摸瓜V3引擎
www.facebook.com	摸瓜V3引擎
star.c10r.facebook.com	摸瓜V3引擎
star-mini.c10r.facebook.com	摸瓜V3引擎
www.apkgalaxylab.com	摸瓜V3引擎

邮箱线索

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=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
签名算法: rsassa_pkcs1v15
有效期自: 2019-08-03 16:45:11+00:00
有效期至: 2049-08-03 16:45:11+00:00
发行人: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android
序列号: 0xcaa46150da4103c2bff3cce38d6d9c78eaefd1d8
哈希算法: sha256
md5值: 25f9eb08c26059876ddc6355e36e313e
sha1值: 7ec16112297bab96361c60977c45dac28646f006
sha256值: 0a0d5f1d97e003e6b2a79ef42d3f00d2ee60dc0ee26b3be408709429da555f77
sha512值: e01a31ff56a144499e2ab1f13c6413c0d190a8453c68ed2c3442180ade492d63c84524bc8aa342548da1d50bafb1ffafc74fdbe91ac595a36f24693bb046f6e1
公钥算法: rsa
密钥长度: 4096
指纹: 5fda72696fba986b5d34cdf2bfb9258fd0a50433687781d6fb46f28488238b61

硬编码敏感信息

可能的敏感信息
"com_facebook_device_auth_instructions" : "Visit facebook.com/device and enter the code shown above."
"firebase_database_url" : "https://galaxylab2019-b0baa.firebaseio.com"
"google_api_key" : "AIzaSyDQjcOLnjy1Edrie_g10ILNTFFfe7LvLu4"
"google_crash_reporting_api_key" : "AIzaSyDQjcOLnjy1Edrie_g10ILNTFFfe7LvLu4"
"sitekey" : "Password"
"com_facebook_device_auth_instructions" : "请访问facebook.com/device并输入以上验证码。"
"[illegible]" : "密码"

"sitekey" : "密码"
"com_facebook_device_auth_instructions" : "facebook.com/deviceにアクセスして、上のコードを入力してください。"
"sitekey" : "パスワード"
"com_facebook_device_auth_instructions" : "facebook.com/device에 방문하여 위 코드를 입력하세요."
"sitekey" : "비밀번호"
"com_facebook_device_auth_instructions" : "Consultez facebook.com/device et entrez le code affiché ci-dessus."
"sitekey" : "Mot de passe"
"com_facebook_device_auth_instructions" : "facebook.com/device adresine git ve yukarıda gösterilen kodu gir."
"sitekey" : "Şifre"
"com_facebook_device_auth_instructions" : "Ve a facebook.com/device e ingresa el código que se muestra arriba."
"sitekey" : "Contraseña"
"com_facebook_device_auth_instructions" : "Откройте facebook.com/device и введите код, показанный выше."
"sitekey" : "Пароль"
"com_facebook_device_auth_instructions" : "前往facebook.com/device</b&gt，並輸入上方顯示的代碼。"
"sitekey" : "密碼"
"sitekey" : "كلمه عبور"

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.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
com.galaxylab.ss.SERVICE	未知	Unknown permission	Unknown permission from android reference
android.permission.FOREGROUND_SERVICE	正常		允许常规应用程序使用 Service.startForeground。
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.RECEIVE_BOOT_COMPLETED	正常	开机时自动启动	允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度
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.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.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。
com.android.vending.BILLING	未知	Unknown permission	Unknown permission from android reference
com.galaxylab.ss.permission.RECEIVE_BROADCASTS	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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.braintreepayments.api.BraintreeBrowserSwitchActivity	Schemes: com.galaxylab.ss.braintree://,