MoGua

SquirrelVPN 1.0.0.APK 分析报告



APP名称: SquirrelVPN

包名:	com.squirrel
域名线索:	11条
URL线索:	15条
邮箱线索:	1条
分析日期:	2024年3月28日
分析平台:	摸瓜反编译平台

文件信息

文件名: SquirrelVPN-Android-1.0.0-168-release.apk
文件大小: 58.94MB
MD5值: 67a685bb538bd20c480199744a0da6a2
SHA1值: 577ae200a152fdfecb35cb36344b110b0f29ebac
SHA256值: f740c17c03c85c6ca80456fa589fe9f688bf6fa416b24a612cd27ccb7bd457b4

APP 信息

App名称: SquirrelVPN
包名: com.squirrel
主活动Activity: com.squirrelvpn.MainActivity
安卓版本名称: 1.0.0
安卓版本: 168

域名线索

域名	服务器信息
pinterest.com	**IP**: 202.160.130.145 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
twitter.com	**IP**: 202.160.128.203 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289670 **经度**: 103.850067
plus.google.com	**IP**: 162.125.2.3 **所属国家**: United States of America **地区**: California

	城市: San Francisco **纬度**: 37.775700 **经度**: -122.395203
api.login.yahoo.com	IP: 74.6.160.138 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
github.com	IP: 20.205.243.166 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
www.facebook.com	IP: 157.240.12.35 **所属国家**: Brazil **地区**: Sao Paulo **城市**: Sao Paulo **纬度**: -23.547501 **经度**: -46.636108
www.example.com	IP: 93.184.216.34 **所属国家**: United States of America **地区**: Virginia **城市**: Ashburn **纬度**: 39.043720 **经度**: -77.487488
ns.adobe.com	没有服务器地理信息.
docs.swmansion.com	IP: 172.67.142.188 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700

	经度: -122.395203
cfg.flurry.com	**IP**: 98.136.147.20 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089
data.flurry.com	**IP**: 69.147.80.15 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.731323 **经度**: -73.990089

URL线索

URL信息	Url所在文件
https://twitter.com/intent/tweet?text=	cl/json/social/TwitterShare.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookPagesManagerShare.java
https://www.facebook.com/sharer/sharer.php?u=	cl/json/social/FacebookShare.java
https://plus.google.com/share?url=	cl/json/social/GooglePlusShare.java
https://pinterest.com/pin/create/button/?url=	cl/json/social/PinterestShare.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/by.java
http://www.example.com	com/flurry/sdk/ed.java

https://data.flurry.com/v1/flr.do	com/flurry/sdk/br.java
https://cfg.flurry.com/sdk/v1/config	com/flurry/sdk/cl.java
https://api.login.yahoo.com/oauth2/device_session	com/flurry/sdk/ef.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenFragment.java
https://github.com/software-mansion/react-native-screens/issues/17	com/swmansion/rnscreens/ScreenStackFragment.java
https://docs.swmansion.com/react-native-gesture-handler/docs/guides/migrating-off-rnghenabledroot	com/swmansion/gesturehandler/react/RNGestureHandlerEnabledRootView.java
https://github.com/rust-lang/rust/issues/39364assertion	lib/armeabi-v7a/libtrunkandroid.so
http://ns.adobe.com/xap/1.0/	lib/armeabi-v7a/libnative-imagetranscoder.so

邮箱线索

邮箱地址	所在文件
appro@openssl.org	lib/arm64-v8a/libtrunkandroid.so

手机线索

签名证书

APK is signed
v1 signature: True
v2 signature: True

v3 signature: False
Found 1 unique certificates
Subject: OU=squirrel, O=wcn, L=Wilmington, ST=Delaware, C=US, CN=www.squirrelvpn.com
Signature Algorithm: rsassa_pkcs1v15
Valid From: 2019-09-18 04:38:44+00:00
Valid To: 2119-08-25 04:38:44+00:00
Issuer: OU=squirrel, O=wcn, L=Wilmington, ST=Delaware, C=US, CN=www.squirrelvpn.com
Serial Number: 0x7840e260
Hash Algorithm: sha256
md5: 65d1e71aa30fc76c3f877f2b2754ab28
sha1: 80a74b7bd096b65ea5b439bce3f05ca7c8a57cf1
sha256: 7e750d7c0297fd1eae69d5cf862badd372c2996ddbfec0fe2961cab6d39f3404
sha512: dd5a68f5ba987e2bb9b67e5196638af29f4edfee241a3e552de9480ef61a67e60b965540127624e0d089608934ec22f3a395b7893ed4ab703e74a7835dfc1706
PublicKey Algorithm: rsa
Bit Size: 2048
Fingerprint: d848f6ccdaacb7206d4f3830f2017ab34230a7c7c27eb4b017c8e28845f31f96

硬编码敏感信息

加壳分析

第三方SDK

名称	分类	URL链接
Flurry	Advertisement, Analytics	https://reports.exodus-privacy.eu.org/trackers/25

此APP的危险动作

	是否危		详细情况

向手机申请的权限	险	类型	
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.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.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.VIBRATE	正常	可控震源	允许应用程序控制振动器
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
com.google.android.c2dm.permission.RECEIVE	合法	C2DM 权限	云到设备消息传递的权限
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.squirrelvpn.MainActivity	Schemes: squirrel://,

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。