



APP线索分析报告

报告由 [摸瓜APP分析平台\(mogua.co\)](http://mogua.co) 生成



 Lite for WhatsApp 2019 1.0.APK

APP名称:	Lite for WhatsApp 2019
包名:	vsv.jugndcmp.liteforwhatsApp2019
域名线索:	4条
URL线索:	4条
邮箱线索:	0条
分析日期:	2022年1月28日 23:05

文件名: liteforwhats546399.apk
文件大小: 3.98MB
MD5值: 47074c23046521dd6bdf6fd2e26524d6
SHA1值: af85825d7e802f694d8a59ed1d29e1adef0000f5
SHA256值: 144b23c7dffa596c159545983003b72a61bc78ca4e974b1a20e4725193f639fd

i APP 信息

App名称: Lite for WhatsApp 2019
包名: vsv.jugndcmp.liteforwhatsApp2019
主活动Activity: vsv.jugndcmp.liteforwhatsApp2019.JUGNDCMP_OneActivity
安卓版本名称: 1.0
安卓版本: 1

🔍 域名线索

域名	是否危险域名	服务器信息
wa.me	good	IP: 157.240.11.53 所属国家: United States of America 地区: California 城市: Los Angeles 纬度: 34.052231 经度: -118.243683 查看地图: Google Map

域名	是否危险域名	服务器信息
capricious-interior.000webhostapp.com	good	IP: 145.14.145.208 所属国家: United States of America 地区: South Carolina 城市: Greenville 纬度: 34.852619 经度: -82.394012 查看地图: Google Map
www.youtube.com	good	IP: 172.217.163.46 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514 查看地图: Google Map
play.google.com	good	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 查看地图: Google Map

URL线索

URL信息	Url所在文件
https://www.youtube.com/watch?v=dBFvNm1Xwq4	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_MainActivity.java

URL信息	Url所在文件
http://play.google.com/store/apps/details?id=	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_MainActivity.java
https://play.google.com/store/apps/details?id=	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_MainActivity.java
https://play.google.com/store/apps/details?id=com.whatsapp	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_Activity_Open_WhatsApp.java
https://wa.me/whatsappphonenumber	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_Activity_Open_WhatsApp.java
https://play.google.com/store/apps/details?id=com.whatsapp	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_Activity_Send_Message.java
https://wa.me/whatsappphonenumber	vsv/jugndcmp/liteforwhatsApp2019/JUGNDCMP_Activity_Send_Message.java
https://play.google.com/store/apps/developer?id=jugnud+Camp	Android String Resource
https://capricious-interior.000webhostapp.com/privacy.html	Android String Resource

☰ 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.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

签名证书

APK is signed

v1 signature: True

v2 signature: True

v3 signature: True

Found 1 unique certificates

Subject: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Signature Algorithm: rsassa_pkcs1v15

Valid From: 2019-09-28 12:37:30+00:00

Valid To: 2049-09-28 12:37:30+00:00

Issuer: C=US, ST=California, L=Mountain View, O=Google Inc., OU=Android, CN=Android

Serial Number: 0xd9f066cee6006c34e567f6ab228d6cb35598de9c

Hash Algorithm: sha256

md5: f6a34ab03c4b46652fc4654ca3ab7b2d

sha1: 54db74ba24bfff9053e9faedb6b8208abcf6ad43

sha256: 421366123504d759dba679bc124957b50d3936817d5d5998cedecbc7d394eb33

sha512: da8ed9c7be460a3cb60130ed25319c40f12e2045f3880b3eb0e417e181e6c8afd84f92927995d94445ac5e70ffdaf4f2a3d01fa0b2f43b647ef371a7a3092592

PublicKey Algorithm: rsa

Bit Size: 4096

Fingerprint: b2303960846f5ccf7601fd65393216dd8cebd29e16f0897cbde8f52d24a61ae5

Exodus威胁情报

名称	分类	URL链接
Google AdMob	Advertisement	https://reports.exodus-privacy.eu.org/trackers/312

加壳分析

文件列表	分析结果	
classes.dex	壳列表	详细情况
	反虚拟机	Build.FINGERPRINT check Build.MODEL check Build.MANUFACTURER check Build.BRAND check Build.DEVICE check Build.PRODUCT check possible VM check
	编译器	r8 without marker (suspicious)

报告由 [摸瓜平台](#) 自动生成，并非包含所有检测结果，有疑问请联系管理员。

[查诈骗APP](#) | [查木马APP](#) | [违法APP分析](#) | [APK代码分析](#)