

# APP线索分析报告 报告由 提瓜APP分析平台(mogua.co) 生成



#### ♣ 新快赚 2.0.12.APK

 APP名称:
 新快赚

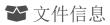
 包名:
 com.yc.wzx

 域名线索:
 44条

 URL线索:
 47条

 邮箱线索:
 0条

分析日期: 2022年1月20日 22:17



文件名: xinkuaizhuan.apk 文件大小: 7.72MB

MD5值: abcfa577d740f48b284a992f24700264

**SHA1**值: 20f7137589d97b10f641d42ee11bcd45e3e7387c

\$HA256值: 5fb2b8a249437526d9a063e4973808340bc5874e9382df14f68ada45f985ce8b

# ▮APP 信息

App名称: 新快赚 包名: com.yc.wzx 主活动**Activity**: com.yc.wzx.view.LoadingActivity 安卓版本名称: 2.0.12 安卓版本:15

### 🔾 域名线索

域名	是否危险域名	服务器信息
u.tn550.com	good	没有服务器地理信息.
hydra.alibaba.com	good	IP: 203.119.169.241  所属国家: China  地区: Beijing  城市: Beijing  纬度: 39.907501  经度: 116.397232  查看地图: Google Map
api.apk22.com	good	没有服务器地理信息.

域名	是否危险域名	服务器信息
sf1-ttcdn-tos.pstatp.com	good	IP: 150.139,249,242 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
i.snssdk.com	good	IP: 140.249.226.225  所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331  经度: 116.997223 查看地图: Google Map
bds-sg.byteoversea.com	good	P: 103.136.220.204 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 査看地图: Google Map
tobapplog.tobsnssdk.com	good	IP: 103.136.220.204 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
www.umeng.com	good	IP: 59.82.29.162 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map
sdfp.snssdk.com	good	IP: 125.35.234.229 所属国家: China 地区: Tianjin 城市: Tianjin 纬度: 39.142220 经度: 117.176666 查看地图: Google Map
tobapplog.ctobsnssdk.com	good	IP: 140.249.89.229 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map

域名	是否危险域名	服务器信息
is,snssdk.com	good	IP: 140.249.225.59 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
xmlpull.org	IP: 74.50.62.60  所属国家: United States of America  地区: Texas  城市: Dallas  纬度: 32.814899  经度: -96.879204  查看地图: Google Map	
mobile.umeng.com	good	IP: 59.82.31.160 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
toblog.itobsnssdk.com	good	IP: 23.37.126.83 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958 查看地图: Google Map
apmlog.snssdk.com	good	IP: 58.49.162.228  所属国家: China 地区: Hubei 城市: Wuhan  纬度: 30.583330  经度: 114.266670  查看地图: Google Map
alogus.umeng.com	good	IP: 106.11.40.44  所属国家: China 地区: Zhejiang 城市: Hangzhou  纬度: 30.293650  经度: 120.161423 查看地图: Google Map
toblog.ctobsnssdk.com	good	IP: 36.102.8.214 所属国家: China 地区: Zhejiang 城市: Hangzhou 纬度: 30.293650 经度: 120.161423 查看地图: Google Map

域名	是否危险域名	服务器信息
ouplog.umeng.com	good	IP: 47.74.172.6 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map
ulogs.umengcloud.com	IP: 106.11.40.44  所属国家: China 地区: Zhejiang 城市: Hangzhou 维度: 30.293650 经度: 120.161423 查看地图: Google Map	
ulogs.umeng.com	good	IP: 203.119.174.133  所属国家: China  地区: Beijing  城市: Beijing  纬度: 39.907501  经度: 116.397232  查看地图: Google Map
127.0.0.1	good	IP: 127.0.0.1  所属国家: - 地区: - 城市: - 纬度: 0.000000  经胺: 0.000000  查看地图: Google Map
cmnsguider.yunos.com	good	IP: 203.119.169.224  所属国家: China  地区: Beijing  城市: Beijing  纬度: 39.907501  经度: 116.397232  查看地图: Google Map
github.com	good	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 查看地图: Google Map
tobapplog.itobsnssdk.com	good	IP: 23.37.126.66  所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958 查看地图: Google Map

域名	是否危险域名	服务器信息
schemas.android.com	good	没有服务器地理信息.
extlog.snssdk.com	good	IP: 140.249.88.207 所属国家: China 地区: Shandong 城市: Jinan 纬度: 36.668331 经度: 116.997223 查看地图: Google Map
bds.snssdk.com	good	IP: 27.185.217.105 所属国家: China 地区: Hebei 城市: Shijiazhuang 纬度: 38.041389 经度: 114.478607 查看地图: Google Map
p3-tt.byteimg.com	good	IP: 218.24.90.185 所属国家: China 地区: Liaoning 城市: Shenyang 纬度: 41.792221 经度: 123.432777 查看地图: Google Map
bds-va.byteoversea.com	good	没有服务器地理信息.
www.chengzijianzhan.com	good	IP: 58.49.193.207 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
sdfp-va.byteoversea.com	good	IP: 23.37.126.65 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958 查看地图: Google Map
success.ctobsnssdk.com	good	IP: 144.123.31.227  所属国家: China 地区: Shandong 城市: Yantai  纬度: 37.533329  经度: 121.400002  查看地图: Google Map

域名	是否危险域名	服务器信息
xml.apache.org	good	IP: 151.101.2.132  所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203 查看地图: Google Map
success.tobsnssdk.com	IP: 103.136.220.204  所属国家: Singapore  地区: Singapore  城市: Singapore  纬度: 1.289670  经度: 103.850067  查看地图: Google Map	
crm.bytedance.com	good	IP: 119.96.66.244 所属国家: China 地区: Hubei 城市: Wuhan 纬度: 30.583330 经度: 114.266670 查看地图: Google Map
log.umsns.com	good	IP: 59.82.31.210 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
sf3-ttcdn-tos.pstatp.com	good	IP: 218.24.90.186  所属国家: China  地区: Liaoning  城市: Shenyang  纬度: 41.792221  经度: 123.432777  查看地图: Google Map
api.weixin.qq.com	good	P: 109.244.145.152   所属国家: China   地区: Beijing   城市: Beijing   纬度: 39.907501   经度: 116.397232   查看地图: Google Map
toblog.tobsnssdk.com	good	P: 103.136.220.204 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289670 经度: 103.850067 查看地图: Google Map

域名	是否危险域名	服务器信息
success.itobsnssdk.com	good	IP: 23.37.126.33 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958 查看地图: Google Map
plbslog.umeng.com	good	IP: 59.82.43.171  所属国家: China  地区: Zhejiang  城市: Hangzhou  纬度: 30.293650  经度: 120.161423  查看地图: Google Map
alogsus.umeng.com	good	IP: 59.82.31.151  所属国家: China  地区: Beijing  城市: Beijing  纬度: 39.907501  经度: 116.397232  查看地图: Google Map
developer.umeng.com	good	IP: 59.82.31.160 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397232 查看地图: Google Map
sdfp-sg.byteoversea.com	good	IP: 23.3.104.53 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689507 经度: 139.691696 查看地图: Google Map

# **₩**URL线索

URL信息	
https://bds.snssdk.com	
https://bds-sg.byteoversea.com	
https://bds-va.byteoversea.com	
https://sdfp.snssdk.com	

URL信息
https://sdfp-sg.byteoversea.com
https://sdfp-va.byteoversea.com
http://u.tn550.com
http://api.apk22.com/d.php?app_name=xiaolin
http://u.tn550.com/agent/index/landing_page?id=374
http://127.0.0.1:
http://p3-tt.byteimg.com/img/web.business.image/201907245d0d495a0568785742e0b940~100x100.image
http://sf3-ttcdn-tos.pstatp.com/obj/mosaic-legacy/2b96e0005c6b6019f8a5b
https://www.chengzijianzhan.com/tetris/page/1639938884171780/? ad.id=1639940885031987&_toutiao_params=%78%22cid%22%3A1639941324071955%2C%22device_id%22%3A38167681029%2C%22log_extra%22%3A%22%7B%5C%22ad_price%5C%22%3A%5C%22XThCVgADKYpdOEjWAAMpijdExKKDLYCp1GNXWw%5C%22%2C%5C%22cc%22cc
http://sf3-ttcdn-tos.pstatp.com/img/mosaic-legacy/2b96e0005c6b6019f8a5b~noop.jpg
https://sf1-ttcdn-tos.pstatp.com/obj/union-fe/playable/97699c8fb31e7836e828cffdd428bc80/index.html?toutiao_card_params=%7B%22name%22%3A%20%22%5Cu5168%5Cu6c11%5Cu6f02%5Cu79fb-3D%5Cu98d9%5Cu8f66%22%2C%20%22pkg_name%22%3A%20%22com.joyfort.merge.car%22%2C%20%22id%22%3A%201639299979328516%2C%20%22download_url%22%3A%20%22https%3A//itunes.apple.com/cn/app/%25E5%2585%25A8%25E6%25B0%2591%25E6%2
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/union_test_tool.mp4
http://sf1-ttcdn-tos.pstatp.com/obj/ttfe/adfe/union_endcard/Lark20190725-175511.png
https://is.snssdk.com/api/ad/union/sdk/get ads/
https://extlog.snssdk.com/service/2/app_log/
https://is.snssdk.com/api/ad/union/dislike_event/
https://is.snssdk.com/api/ad/union/sdk/reward_video/reward/
https://is.snssdk.com/union/service/sdk/upload/v2/
https://is.snssdk.com/api/ad/union/sdk/material/check/
https://is.snssdk.com/api/ad/union/sdk/stats/batch/
https://i.snssdk.com/inspect/aegis/client/page/
https://sf3-ttcdn-tos.pstatp.com/obj/ad-pattern/renderer/package.json
https://i.snssdk.com/api/ad/union/sdk/stats/
https://is.snssdk.com/api/ad/union/sdk/upload/app_info/

URL信息
https://is.snssdk.com/api/ad/union/sdk/settings/
http://apmlog.snssdk.com/apm/collect/crash/
https://toblog.ctobsnssdk.com
https://tobapplog.ctobsnssdk.com
https://toblog.tobsnssdk.com
https://tobapplog.tobsnssdk.com
https://toblog.itobsnssdk.com
https://tobapplog.itobsnssdk.com
https://toblog.ctobsnssdk.com/service/2/device_register_only/
https://toblog.ctobsnssdk.com/service/2/app_alert_check/
https://toblog.ctobsnssdk.com/service/2/log_settings/
https://toblog.ctobsnssdk.com/service/2/abtest_config/
https://success.ctobsnssdk.com
https://toblog.tobsnssdk.com/service/2/device_register_only/
https://toblog.tobsnssdk.com/service/2/app_alert_check/
https://toblog.tobsnssdk.com/service/2/log_settings/
https://toblog.tobsnssdk.com/service/2/abtest_config/
https://success.tobsnssdk.com
https://toblog.itobsnssdk.com/service/2/device_register_only/
https://toblog.itobsnssdk.com/service/2/app_alert_check/
https://toblog.itobsnssdk.com/service/2/log_settings/
https://toblog.itobsnssdk.com/service/2/abtest_config/
https://success.itobsnssdk.com
https://plbslog.umeng.com
https://ouplog.umeng.com
https://developer.umeng.com/docs/66632/detail/

URL信息
https://ulogs.umeng.com/unify_logs
https://ulogs.umengcloud.com/unify_logs
https://alogus.umeng.com/unify_logs
https://alogsus.umeng.com/unify_logs
https://cmnsguider.yunos.com:443/genDeviceToken
http://developer.umeng.com/docs/66650/cate/66650
https://mobile.umeng.com/images/pic/home/social/img-1.png
https://log.umsns.com/
https://log.umsns.com/
https://log.umsns.com/
https://log.umsns.com/link/qq/download/
https://log.umsns.com/link/weixin/download/
http://www.umeng.com/social
https://developer.umeng.com/docs/66632/detail/
https://api.weixin.qq.com/sns/oauth2/access_token?
https://api.weixin.qq.com/sns/oauth2/refresh_token?
https://api.weixin.qq.com/sns/userinfo?access_token=
https://api.weixin.qq.com/sns/oauth2/refresh_token?appid=
http://xmlpull.org/v1/doc/features.html#indent-output
http://xmlpull.org/v1/doc/features.html#indent-output
http://hydra.alibaba.com/
http://xml.apache.org/xslt\tindent-amount
https://crm.bytedance.com/audit/inspect/client/app/resend/
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins
https://github.com/ReactiveX/RxJava/wiki/Plugins

#### URL信息

https://github.com/ReactiveX/RxJava/wiki/Plugins

https://github.com/ReactiveX/RxJava/wiki/Plugins

https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0#error-handling

https://github.com/ReactiveX/RxJava/wiki/Error-Handling

http://schemas.android.com/apk/res/android

http://schemas.android.com/apk/res/android

http://schemas.android.com/apk/res/android

# ■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.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.RECEIVE_USER_PRESENT	未知	Unknown permission	Unknown permission from android reference
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.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.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.ACCESS_FINE_LOCATION	危险	精细定位(GPS)	访问精细位置源,例如手机上的全球定位系统,如果可用。恶意应用程序可以使用它来确定您的位置,并可能消耗额外的电池电量
android.permission.ACCESS_COARSE_LOCATION	危险	粗定位	访问粗略位置源,例如移动网络数据库,以确定大概的电话位置(如果可用)。恶意应用程序可以使用它来确定您的大致位置
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.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.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.WRITE_SETTINGS	危险	修改全局系统设置	允许应用程序修改系统设定数据。恶意应用可能会损坏你的系统的配置。
android.permission.RESTART_PACKAGES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.BROADCAST_STICKY	正常	发送粘性广播	允许应用程序发送粘性广播,在广播结束后保留。恶意应用程序会导致手机使用过多内存,从而使手机运行缓慢或不稳定

向手机申请的权限	是否危险	类型	详细情况
android.permission.KILL_BACKGROUND_PROCESSES	正常	杀死后台进程	允许应用程序杀死其他应用程序的后台进程,即使内存不低
android.permission.GET_TASKS	危险	检索正在运行的应用程序	允许应用程序检索有关当前和最近运行的任务的信息。可能允许恶意应用程序发现有关其他应用程序的私人信息
android.permission.READ_LOGS	危险	读取敏感日志数据	允许应用程序从系统读小号各种日志文件。这使它能够发现有关您使用手机做什么的一般信息,可能包括个人或私人信息
android.permission.BLUETOOTH	正常	创建蓝牙连接	允许应用程序连接到配对的蓝牙设备
android.permission.BATTERY_STATS	合法	修改电池统计信息	允许修改收集的电池统计信息。不供普通应用程序使用
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



APK is signed

v1 signature: True

v2 signature: False v3 signature: False

Found 1 unique certificates

Subject: OU=CN

Signature Algorithm: rsassa\_pkcs1v15 Valid From: 2018-11-23 10:42:15+00:00 Valid To: 2043-11-17 10:42:15+00:00

Issuer: OU=CN

Serial Number: 0x43b32de8 Hash Algorithm: sha256

md5: 71136b4a93d985c696f164f7d60daa72

sha1: 065b45d614b0724b23b08a908cd4a6753e6cddcc

sha256: 40577d3037fb0eb8d7901dc6d94d9dc5655efb3956c0e689c8363584a9cc558a

sha512:30123e4d145c032103784ba343d97f50f17676f73588e2f9fa2ebf6ebdcc29046a4062a0db3e75d71e290aac811fca5117e66ff89c9dd1fc9109ad9ac6978664

# **在 Exodus**威胁情报

名称	分类	URL链接
Pangle	Advertisement	https://reports.exodus-privacy.eu.org/trackers/363

## **命** 加壳分析

文件列表	分析结果
------	------

文件列表	分析结果
classes.dex	克列表 详细情况  Description    Description    Build.MANUFACTURER check possible Build.SERIAL check SIM operator check network operator name check
	编译器 r8 without marker (suspicious)
	売列表 详细情况
classes2.dex	Build.FINGERPRINT check Build.MANUFACTURER check Build.HARDWARE check Build.BOARD check possible Build.SERIAL check Build.TAGS check SIM operator check network operator name check subscriber ID check  ##
	High Hair To Without marker (suspicious)
lib/arm64-v8a/libnms.so	売列表       详细情况         模糊器       ByteGuard 0.9.3
lib/armeabi-v7a/libnms.so	売列表       详细情况         模糊器       ByteGuard 0.9.3
lib/armeabi/libnms.so	売列表   详细情况     模糊器   ByteGuard 0.9.3
lib/x86/libnms.so	売列表         详细情况           模糊器         ByteGuard 0.9.3

文件列表	分析结果	
lib/x86_64/libnms.so	売列表	详细情况
IID/X00_04/IIDHIIIS.SU	模糊器	ByteGuard 0.9.3

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