MoGua

Hunter 6.21.APK 分析报告

APP名称: Hunter

包名:	com.zhenxi.hunter
域名线索:	20条
URL线索:	24条
邮箱线索:	1条
分析日期:	2025年6月28日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: Hunter_6.21.apk
文件大小: 11.84MB
MD5值: bdb2ad0c83c793e4258b285dc4d6838a
SHA1值: 20797e59eb7c0e92d4cfec0c2a4421e5e595f977
SHA256值: 46f2050b73481ecdfc0e0871816c5801bc4aecf0be244177f6324c53628249d2

APP 信息

App名称: Hunter
包名: com.zhenxi.hunter
主活动Activity: com.zhenxi.hunter.MainActivity
安卓版本名称: 6.21
安卓版本: 621

域名线索

域名	服务器信息
www.recaptcha.net	**IP**: 114.250.64.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
firebase-settings.crashlytics.com	**IP**: 114.250.65.34 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
firebaseinstallations.googleapis.com	**IP**: 142.251.215.234 **所属国家**: United States of America **地区**: California

	城市: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.googleadservices.com	**IP**: 114.250.63.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
accounts.google.com	**IP**: 93.46.8.90 **所属国家**: Italy **地区**: Lombardia **城市**: Milan **纬度**: 45.464336 **经度**: 9.188547
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
goo.gl	**IP**: 142.250.73.78 **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**: 114.250.70.33 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102

firebase.google.com	**IP**: 142.250.73.142 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
youtrack.jetbrains.com	**IP**: 63.35.30.167 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
google.com	**IP**: 59.24.3.174 **所属国家**: Korea (Republic of) **地区**: Gyeonggi-do **城市**: Seongnam **纬度**: 37.420624 **经度**: 127.126717
pagead2.googlesyndication.com	**IP**: 114.250.64.38 **所属国家**: China **地区**: Beijing **城市**: Beijing **纬度**: 39.907501 **经度**: 116.397102
android.googlesource.com	**IP**: 108.177.98.82 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
plus.google.com	**IP**: 65.49.26.97 **所属国家**: United States of America **地区**: Missouri **城市**: Saint Louis

	纬度: 38.655479 **经度**: -90.452339
schemas.android.com	没有服务器地理信息.
issuetracker.google.com	**IP**: 142.250.217.110 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
firebaseappcheck.googleapis.com	**IP**: 142.250.73.106 **所属国家**: United States of America **地区**: California **城市**: Mountain View **纬度**: 37.405991 **经度**: -122.078514
www.apache.org	**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
kubernetes.io	**IP**: 147.75.40.148 **所属国家**: United States of America **地区**: New York **城市**: New York City **纬度**: 40.713516 **经度**: -74.008041
www.google.com	**IP**: 157.240.17.35 **所属国家**: Switzerland **地区**: Zurich **城市**: Zurich **纬度**: 47.366825 **经度**: 8.549790

URL线索

URL信息	Url所在文件
https://plus.google.com/	YouAreLoser/FW.java
https://pagead2.googlesyndication.com/pagead/gen_204?id=gmob-apps	YouAreLoser/C0918fS.java
https://github.com/google/gson/blob/main/Troubleshooting.md	YouAreLoser/C2138zs.java
https://app-measurement.com/a	YouAreLoser/QT.java
https://app-measurement.com/s/d	YouAreLoser/QT.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	YouAreLoser/C1108ig.java
https://github.com/google/gson/blob/main/Troubleshooting.md	YouAreLoser/PC.java
https://github.com/google/gson/blob/main/Troubleshooting.md	YouAreLoser/VC.java
http://schemas.android.com/apk/res/android	YouAreLoser/QP.java
https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0	YouAreLoser/QP.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	YouAreLoser/C0077Dg.java
https://accounts.google.com/o/oauth2/revoke?token=	YouAreLoser/MR.java
https://github.com/google/gson/blob/main/Troubleshooting.md	YouAreLoser/ZL.java
https://github.com/ReactiveX/RxJava/wiki/Error-Handling	YouAreLoser/C0637am.java

https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/	YouAreLoser/C0370Qb.java
https://firebase.google.com/docs/crashlytics/get-started?platform=android	YouAreLoser/C0370Qb.java
https://firebase.google.com/support/guides/disable-analytics	YouAreLoser/XT.java
https://goo.gl/NAOOOI.	YouAreLoser/C1879vW.java
https://goo.gl/NAOOOI	YouAreLoser/C1879vW.java
https://firebaseinstallations.googleapis.com/v1/	YouAreLoser/C0935fm.java
https://issuetracker.google.com/issues/241760537	YouAreLoser/QM.java
https://firebase.google.com/support/privacy/init-options.	YouAreLoser/C1114im.java
https://issuetracker.google.com/issues/new?component=907884&template=1466542	YouAreLoser/C1167jg.java
https://www.google.com	YouAreLoser/C1.java
https://google.com/search?	YouAreLoser/RunnableC1041hV.java
https://firebaseappcheck.googleapis.com/v1/projects/	YouAreLoser/CallableC0479Uu.java
https://www.googleadservices.com/pagead/conversion/app/deeplink?id_type=adid&sdk_version=	YouAreLoser/C0742cV.java
https://youtrack.jetbrains.com/issue/KT-46465	摸瓜V3引擎
https://app-measurement.com/s/d	摸瓜V3引擎
https://app-measurement.com/a	摸瓜V3引擎
http://schemas.android.com/apk/res/android	摸瓜V3引擎
https://www.recaptcha.net/recaptcha/api3	摸瓜V3引擎

https://android.googlesource.com/toolchain/llvm-project	摸瓜V3引擎
http://schemas.android.com/aapt	摸瓜V3引擎
https://developer.android.com/google/play/integrity/reference/com/google/android/play/core/integrity	摸瓜V3引擎
http://schemas.android.com/apk/res-auto	摸瓜V3引擎
https://kubernetes.io/docs/tasks/access-kubernetes-api/custom-resources/custom-resource-definitions/	摸瓜V3引擎
http://www.apache.org/licenses/LICENSE-2.0	摸瓜V3引擎

邮箱线索

邮箱地址	所在文件
u0013android@android.com0 u0013android@android.com	YouAreLoser/HT.java

手机线索

手机号	所在文件
15552000000	YouAreLoser/C1279lV.java

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=1, ST=1, L=1, O=1, OU=1, CN=1
签名算法: rsassa_pkcs1v15
有效期自: 2018-01-13 12:19:56+00:00
有效期至: 2043-01-07 12:19:56+00:00
发行人: C=1, ST=1, L=1, O=1, OU=1, CN=1
序列号: 0x785fb134
哈希算法: sha256
md5值: 81b7916b384fbfb3b2df6c9a3cbb5774
sha1值: 2625712e6895e5512eb1f5782ff4e3a3e4bfbc2d
sha256值: 4f32a42eff70ac87b85ab4c30bd732f413b54bd74f41c9c002d154acc08ecb1a
sha512值: 50fa339db355d87231a2dfc00152a08cdeefbd29e0a4caa8e2ed2855a0da7cf31ce5c1bc445bfe811ae2f5343bff2e8aab7df842c1c978d63eb0108dfd903633
公钥算法: rsa
密钥长度: 2048
指纹: 454c15a7fa7bbff75d4f0862947fc8a34dc40965b0db0f4af95e046d8e8bb0c0

硬编码敏感信息

可能的敏感信息
"com.google.firebase.crashlytics.mapping_file_id" : "e21f98fd427741778fff33cb00f6c00b"
"google_api_key" : "AIzaSyDgu9y3NQTiQOYgKSpOt-VtLSXNNDjgN6U"
"google_crash_reporting_api_key" : "AIzaSyDgu9y3NQTiQOYgKSpOt-VtLSXNNDjgN6U"

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.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.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.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.SYSTEM_ALERT_WINDOW	危险	显示系统级警报	允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕

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_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.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.xiaomi.security.permission.ACCESS_XSOF	未知	Unknown permission	Unknown permission from android reference
android.permission.INSTALL_PACKAGES	系统需要	直接安装应用程序	允许应用程序安装新的或更新的 Android 包。恶意应用程序可以使用它来添加具有任意强大权限的新应用程序
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.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.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.gms.permission.AD_ID	未知	Unknown permission	Unknown permission from android reference
android.permission.ACCESS_ADSERVICES_ATTRIBUTION	未知	Unknown permission	Unknown permission from android reference

android.permission.ACCESS_ADSERVICES_AD_ID	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.providers.gsf.permission.READ_GSERVICES	未知	Unknown permission	Unknown permission from android reference
com.zhenxi.hunter.DYNAMIC_RECEIVER_NOT_EXPORTED_PERMISSION	未知	Unknown permission	Unknown permission from android reference

应用内通信

活动(ACTIVITY)	**通信**(INTENT)
com.google.firebase.auth.internal.GenericIdpActivity	Schemes: genericidp://, Hosts: firebase.auth, Paths: /,
com.google.firebase.auth.internal.RecaptchaActivity	Schemes: recaptcha://, Hosts: firebase.auth, Paths: /,

---