南明离火
移动应用检测平台

ANDROID 静态分析报告

Via • v6.3.1

分析日期: 2025-04-15 17:59:57

应用概览

文件名称:	Via-6.3.1-20250228-14736去白.apk
文件大小:	2.39MB
应用名称:	Via
软件包名:	mark.via
主活动:	mark.via.Shell
版本号:	6.3.1
最小SDK:	14
目标SDK:	35
加固信息:	未加壳
开发框架:	Java/Kotlin
应用程序安全分数:	49/100 (中风险)
跟踪器检测:	2/432
杀软检测:	2 个杀毒软件报毒
MD5:	2b6b045d4d6cd7dbc1e0531d0857eb05
SHA1:	8d15ec5028bb457a0e02252edc8112220e7b3057
SHA256:	5084c03116d374d31762d7fdbd18bfabfb878e29ed16305179c42b765babe3f8

分析结果严重性

高危	中危	信息	安全	关注
3	18	2	2	50

四大组件信息

Activity组件：3个，其中export的有： 2个
Service组件：7个，其中export的有： 0个
Receiver组件：3个，其中export的有： 1个
Provider组件：1个，其中export的有： 0个

证书信息

二进制文件已签名
v1 签名: True
v2 签名: True
v3 签名: True
v4 签名: False
主题: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
签名算法: rsassa_pkcs1v15
有效期自: 2008-02-29 01:33:46+00:00
有效期至: 2035-07-17 01:33:46+00:00
发行人: C=US, ST=California, L=Mountain View, O=Android, OU=Android, CN=Android, E=android@android.com
序列号: 0x936eacbe07f201df
哈希算法: sha1
证书MD5: e89b158e4bcf988ebd09eb83f5378e87
证书SHA1: 61ed377e85d386a8dfee6b864bd85b0bfaa5af81
证书SHA256: a40da80a59d170caa950cf15c18c454d47a39b26989d8b640ecd745ba71bf5dc
证书SHA512:
5216ccb62004c4534f35c780ad7c582f4ee528371e27d4151f0553325de9ccbe6b34ec4233f5f640703581053abfea303977272d17958704d89b7711292a4569

公钥算法: rsa
密钥长度: 2048
指纹: f9f32662753449dc550fd88f1ed90e94b81adef9389ba16b89a6f3579c112e75
找到 1 个唯一证书

应用权限

权限名称	安全等级	权限内容	权限描述
mark.via.permission.BROADCAST	未知	未知权限	来自 android 引用的未知权限。
android.permission.ACCESS_NETWORK_STATE	普通	获取网络状态	允许应用程序查看所有网络的状态。
android.permission.ACCESS_WIFI_STATE	普通	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	危险	完全互联网访问	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.WAKE_LOCK	危险	防止手机休眠	允许应用程序防止手机休眠，在手机屏幕关闭后后台进程仍然运行。
android.permission.ACCESS_FINE_LOCATION	危险	获取精确位置	通过GPS芯片接收卫星的定位信息，定位精度达10米以内。恶意程序可以用它来确定您所在的位置。
android.permission.ACCESS_COARSE_LOCATION	危险	获取粗略位置	通过WiFi或移动基站的方式获取用户粗略的经纬度信息，定位精度大概误差在30~1500米。恶意程序可以用它来确定您的大概位置。
android.permission.REQUEST_INSTALL_PACKAGES	危险	允许安装应用程序	Android8.0 以上系统允许安装未知来源应用程序权限。
android.permission.FOREGROUND_SERVICE	普通	创建前台Service	Android 9.0以上允许常规应用程序使用 Service.startForeground，用于podcast播放（推送悬浮播放，锁屏播放）
android.permission.QUERY_ALL_PACKAGES	普通	获取已安装应用程序列表	Android 11引入与包可见性相关的权限，允许查询设备上的任何普通应用程序，而不考虑清单声明。
android.permission.POST_NOTIFICATIONS	危险	发送通知的运行时权限	允许应用发布通知，Android 13 引入的新权限。
android.permission.RECORD_AUDIO	危险	获取录音权限	允许应用程序获取录音权限。

android.permission.MODIFY_AUDIO_SETTINGS	危险	允许应用修改全局音频设置	允许应用程序修改全局音频设置，如音量。多用于消息语音功能。
android.permission.VIBRATE	普通	控制振动器	允许应用程序控制振动器，用于消息通知振动功能。
com.android.launcher.permission.INSTALL_SHORTCUT	签名	创建快捷方式	这个权限是允许应用程序创建桌面快捷方式。
com.bbk.launcher2.permission.READ_SETTINGS	未知	未知权限	来自 android 引用的未知权限。
android.permission.FOREGROUND_SERVICE_DATA_SYNC	普通	允许前台服务进行数据同步	允许常规应用程序使用类型为“dataSync”的 Service.startForeground。
android.permission.FOREGROUND_SERVICE_MEDIA_PLAYBACK	普通	启用用于媒体播放的前台服务	允许常规应用程序使用类型为“mediaPlayback”的 Service.startForeground。
android.permission.CAMERA	危险	拍照和录制视频	允许应用程序拍摄照片和视频，且允许应用程序收集相机在任何时候拍到的图像
com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE	普通	Google 定义的权限	由 Google 定义的自定义权限。
com.google.android.gms.permission.AD_ID	普通	应用程序显示广告	此应用程序使用 Google 广告 ID，并且可能会投放广告。

可浏览的Activity组件

ACTIVITY	INTENT
mark.via.Shell	Schemes: http://, https://, about://, javascript://, via://, inline://, file://, content://, Mime Types: text/html, text/plain, application/xhtml+xml, application/vnd.wap.xhtml+xml,

网络通信安全

高危: **2** | 警告: **1** | 信息: **0** | 安全: **0**

序号	范围	严重级别	描述
1	*	高危	基本配置不安全地配置为允许到所有域的明文流量。
2	*	警告	基本配置配置为信任系统证书。
3	*	高危	基本配置配置为信任用户安装的证书。

证书安全分析

高危: **0** | 警告: **1** | 信息: **1**

标题	严重程度	描述信息
已签名应用	信息	应用程序使用代码签名证书进行签名

MANIFEST分析

高危: **1** | 警告: **6** | 信息: **0** | 屏蔽: **0**

序号	问题	严重程度	描述信息

1	应用程序已启用明文网络流量 [android:usesCleartextTraffic=true]	警告	应用程序打算使用明文网络流量，例如明文HTTP，FTP协议，DownloadManager和MediaPlayer。针对API级别27或更低的应用程序，默认值为“true”。针对API级别28或更高的应用程序，默认值为“false”。避免使用明文流量的主要原因是缺乏机密性，真实性和防篡改保护；网络攻击者可以窃听传输的数据，并且可以在不被检测到的情况下修改它。
2	应用程序具有网络安全配置 [android:networkSecurityConfig=@xml/e]	信息	网络安全配置功能让应用程序可以在一个安全的，声明式的配置文件中自定义他们的网络安全设置，而不需要修改应用程序代码。这些设置可以针对特定的域名和特定的应用程序进行配置。
3	应用程序数据可以被备份 [android:allowBackup=true]	警告	这个标志允许任何人通过adb备份你的应用程序数据。它允许已经启用了USB调试的用户从设备上复制应用程序数据。
4	Activity (mark.via.Shell) 的启动模式不是standard模式	高危	Activity 不应将启动模式属性设置为 "singleTask/singleInstance"，因为这会使其成为根 Activity，并可能导致其他应用程序读取调用 Intent 的内容。因此，当 Intent 包含敏感信息时，需要使用 "standard" 启动模式属性。
5	Activity设置了TaskAffinity属性 (mark.via.Trampoline)	警告	如果设置了 taskAffinity，其他应用程序可能会读取发送到属于另一个任务的 Activity 的 Intent。为了防止其他应用程序读取发送或接收的 Intent 中的敏感信息，请始终使用默认设置，将 affinity 保持为包名
6	Activity (mark.via.Trampoline) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
7	Activity (mark.via.Search) 未被保护。 [android:exported=true]	警告	发现 Activity与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。
8	Broadcast Receiver (mark.via.widget.SearchWidgetProvider) 未被保护。 [android:exported=true]	警告	发现 Broadcast Receiver与设备上的其他应用程序共享，因此可被设备上的任何其他应用程序访问。

</> 安全漏洞检测

高危: **0** | 警告: **9** | 信息: **2** | 安全: **2** | 屏蔽: **0**

序号	问题	等级	参考标准	文件位置
1	此应用程序使用SSL Pinning 来检测或防止安全通信通道中的MITM攻击	安全	OWASP MASVS: MSTG-NETWORK-4	升级会员：解锁高级权限
2	应用程序记录日志信息,不得记录敏感信息	信息	CWE: CWE-532: 通过日志文件的信息暴露 OWASP MASVS: MSTG-STORAGE-3	升级会员：解锁高级权限
3	此应用程序可能具有Root检测功能	安全	OWASP MASVS: MSTG-RESILIENCE-1	升级会员：解锁高级权限
4	MD5是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限

5	应用程序使用不安全的随机数生成器	警告	CWE: CWE-330: 使用不充分的随机数 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-6	升级会员：解锁高级权限
6	应用程序使用SQLite数据库并执行原始SQL查询。原始SQL查询中不受信任的用户输入可能会导致SQL注入。敏感信息也应加密并写入数据库	警告	CWE: CWE-89: SQL命令中使用的特殊元素转义处理不恰当（'SQL 注入'） OWASP Top 10: M7: Client Code Quality	升级会员：解锁高级权限
7	不安全的Web视图实现。可能存在WebView任意代码执行漏洞	警告	CWE: CWE-749: 暴露危险方法或函数 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
8	SHA-1是已知存在哈希冲突的弱哈希	警告	CWE: CWE-327: 使用了破损或被认为是不安全的加密算法 OWASP Top 10: M5: Insufficient Cryptography OWASP MASVS: MSTG-CRYPTO-4	升级会员：解锁高级权限
9	应用程序可以读取/写入外部存储器，任何应用程序都可以读取写入外部存储器的数据	警告	CWE: CWE-276: 默认权限不正确 OWASP Top 10: M2: Insecure Data Storage OWASP MASVS: MSTG-STORAGE-2	升级会员：解锁高级权限
10	文件可能包含硬编码的敏感信息，如用户名、密码、密钥等	警告	CWE: CWE-312: 明文存储敏感信息 OWASP Top 10: M9: Reverse Engineering OWASP MASVS: MSTG-STORAGE-14	升级会员：解锁高级权限
11	此应用程序将数据复制到剪贴板。敏感数据不应复制到剪贴板，因为其他应用程序可以访问它	信息	OWASP MASVS: MSTG-STORAGE-10	升级会员：解锁高级权限
12	可能存在跨域漏洞。在 WebView 中启用从 URL 访问文件可能会泄漏文件系统中的敏感信息	警告	CWE: CWE-200: 信息泄露 OWASP Top 10: M1: Improper Platform Usage OWASP MASVS: MSTG-PLATFORM-7	升级会员：解锁高级权限
13	IP地址泄露	警告	CWE: CWE-200: 信息泄露 OWASP MASVS: MSTG-CODE-2	升级会员：解锁高级权限

行为分析

编号	行为	标签	文件
00013	读取文件并将其放入流中	文件	升级会员：解锁高级权限
00183	获取当前相机参数并更改设置	相机	升级会员：解锁高级权限
00096	连接到 URL 并设置请求方法	命令 网络	升级会员：解锁高级权限
00089	连接到 URL 并接收来自服务器的输入流	命令 网络	升级会员：解锁高级权限
00030	通过给定的 URL 连接到远程服务器	网络	升级会员：解锁高级权限
00109	连接到 URL 并获取响应代码	网络 命令	升级会员：解锁高级权限
00192	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00063	隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00014	将文件读入流并将其放入 JSON 对象中	文件	升级会员：解锁高级权限
00022	从给定的文件绝对路径打开文件	文件	升级会员：解锁高级权限
00005	获取文件的绝对路径并将其放入 JSON 对象	文件	升级会员：解锁高级权限
00004	获取文件名并将其放入 JSON 对象	文件 信息收集	升级会员：解锁高级权限
00015	将缓冲流（数据）放入 JSON 对象	文件	升级会员：解锁高级权限
00123	连接到远程服务器后将响应保存为 JSON	网络 命令	升级会员：解锁高级权限
00163	创建新的 Socket 并连接到它	socket	升级会员：解锁高级权限
00094	连接到 URL 并从中读取数据	命令 网络	升级会员：解锁高级权限
00108	从给定的 URL 读取输入流	网络 命令	升级会员：解锁高级权限
00053	监视给定内容 URI 标识的数据更改（SMS、MMS 等）	短信	升级会员：解锁高级权限
00011	从 URI 查询数据（SMS、CALLLOGS）	短信 通话记录 信息收集	升级会员：解锁高级权限
00054	从文件安装其他APK	反射	升级会员：解锁高级权限
00012	读取数据并放入缓冲流	文件	升级会员：解锁高级权限
00072	将 HTTP 输入流写入文件	命令 网络 文件	升级会员：解锁高级权限
00162	创建 InetSocketAddress 对象并连接到它	socket	升级会员：解锁高级权限

00024	Base64解码后写入文件	反射 文件	升级会员：解锁高级权限
00189	获取短信内容	短信	升级会员：解锁高级权限
00188	获取短信地址	短信	升级会员：解锁高级权限
00200	从联系人列表中查询数据	信息收集 联系人	升级会员：解锁高级权限
00201	从通话记录中查询数据	信息收集 通话记录	升级会员：解锁高级权限
00077	读取敏感数据（短信、通话记录等）	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00187	查询 URI 并检查结果	信息收集 短信 通话记录 日历	升级会员：解锁高级权限
00036	从 res/raw 目录获取资源文件	反射	升级会员：解锁高级权限
00125	检查给定的文件路径是否存在	文件	升级会员：解锁高级权限
00091	从广播中检索数据	信息收集	升级会员：解锁高级权限
00009	将游标中的数据放入JSON对象	文件	升级会员：解锁高级权限
00191	获取短信收件箱中的消息	短信	升级会员：解锁高级权限
00056	修改语音音量	控制	升级会员：解锁高级权限
00051	通过setData隐式意图（查看网页、拨打电话等）	控制	升级会员：解锁高级权限
00173	获取 AccessibilityNodeInfo 屏幕中的边界并执行操作	无障碍服务	升级会员：解锁高级权限

敏感权限分析

类型	匹配	权限
恶意软件常用权限	8/30	android.permission.WAKE_LOCK android.permission.ACCESS_FINE_LOCATION android.permission.ACCESS_COARSE_LOCATION android.permission.REQUEST_INSTALL_PACKAGES android.permission.RECORD_AUDIO android.permission.MODIFY_AUDIO_SETTINGS android.permission.VIBRATE android.permission.CAMERA

其它常用权限	8/46	android.permission.ACCESS_NETWORK_STATE android.permission.ACCESS_WIFI_STATE android.permission.INTERNET android.permission.WRITE_EXTERNAL_STORAGE android.permission.FOREGROUND_SERVICE com.android.launcher.permission.INSTALL_SHORTCUT com.google.android.finsky.permission.BIND_GET_INSTALL_REFERRER_SERVICE com.google.android.gms.permission.AD_ID

常用: 已知恶意软件广泛滥用的权限。

其它常用权限: 已知恶意软件经常滥用的权限。

域名检测

域名	状态	中国境内	位置信息
us-c.viayoo.com	安全	否	**IP地址:** 104.21.16.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
file-examples.com	安全	否	**IP地址:** 104.21.16.1 **国家:** 波兰 **地区:** 大波兰省 **城市:** 波兹南 **纬度:** 52.406914 **经度:** 16.930000 **查看:** Google 地图
www.huanqiu.com	安全	是	**IP地址:** 58.222.30.203 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
weibo.com	安全	是	**IP地址:** 104.21.16.1 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.xs8.cn	安全	是	**IP地址:** 36.99.172.202 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图

beian.miit.gov.cn	安全	是	**IP地址:** 36.99.172.202 **国家:** 中国 **地区:** 河北 **城市:** 廊坊 **纬度:** 39.509720 **经度:** 116.694717 **查看:** 高德地图
us.app.viayoo.com	安全	否	**IP地址:** 121.229.94.194 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 洛杉矶 **纬度:** 34.052570 **经度:** -118.243904 **查看:** Google 地图
st.so.com	安全	是	**IP地址:** 180.163.251.253 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.oschina.net	安全	是	**IP地址:** 180.76.198.147 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
help.eyeo.com	安全	否	**IP地址:** 34.160.31.169 **国家:** 美国 **地区:** 密苏里州 **城市:** 堪萨斯城 **纬度:** 39.099731 **经度:** -94.578568 **查看:** Google 地图
www.cn-healthcare.com	安全	是	**IP地址:** 60.205.173.130 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
wormhole.app	安全	否	**IP地址:** 104.26.6.129 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
sug.so.360.cn	安全	是	**IP地址:** 36.99.172.202 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图

www.360doc.cn	安全	是	**IP地址:** 36.99.172.202 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
lingva.retiolus.net	安全	否	**IP地址:** 80.67.181.209 **国家:** 比利时 **地区:** 布鲁塞尔首都大区市镇 **城市:** 布鲁塞尔 **纬度:** 50.850849 **经度:** 4.348780 **查看:** Google 地图
wap.sogou.com	安全	是	**IP地址:** 121.229.94.194 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
app.viayoo.com	安全	是	**IP地址:** 47.96.219.181 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
www.hupu.com	安全	是	**IP地址:** 47.103.37.234 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
c.viayoo.com	安全	是	**IP地址:** 47.103.37.234 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.guanha.cn	安全	是	**IP地址:** 180.97.228.82 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
raw.githubusercontent.com	安全	否	**IP地址:** 185.199.109.133 **国家:** 美国 **地区:** 宾夕法尼亚 **城市:** 加利福尼亚 **纬度:** 40.065647 **经度:** -79.891724 **查看:** Google 地图

www.zhihu.com	安全	是	**IP地址:** 47.103.37.234 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
iqdb.org	安全	否	**IP地址:** 91.121.210.31 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图
yandex.com	安全	否	**IP地址:** 104.26.4.72 **国家:** 俄罗斯联邦 **地区:** 莫斯科 **城市:** 莫斯科 **纬度:** 55.752258 **经度:** 37.615471 **查看:** Google 地图
www.10099.com.cn	安全	是	**IP地址:** 120.39.197.140 **国家:** 中国 **地区:** 福建 **城市:** 三明 **纬度:** 26.248610 **经度:** 117.618607 **查看:** 高德地图
www.ccopyright.com.cn	安全	是	**IP地址:** 180.97.168.71 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.hao123.com	安全	是	**IP地址:** 180.97.107.108 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
api.bing.com	安全	否	**IP地址:** 49.7.36.23 **国家:** 美国 **地区:** 华盛顿 **城市:** 雷德蒙 **纬度:** 47.682899 **经度:** -122.120903 **查看:** Google 地图
www.jd.com	安全	是	**IP地址:** 121.226.246.3 **国家:** 中国 **地区:** 江苏 **城市:** 宿迁 **纬度:** 33.933334 **经度:** 118.283333 **查看:** 高德地图

goo.gl	安全	否	**IP地址:** 104.26.4.72 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
dav.jianguoyun.com	安全	是	**IP地址:** 58.215.175.52 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
pagead2.googlesyndication.com	安全	是	**IP地址:** 180.163.151.166 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.gushiwen.cn	安全	是	**IP地址:** 58.215.157.239 **国家:** 中国 **地区:** 江苏 **城市:** 无锡 **纬度:** 31.569349 **经度:** 120.288788 **查看:** 高德地图
www.guoxuedashi.net	安全	是	**IP地址:** 58.218.199.86 **国家:** 中国 **地区:** 江苏 **城市:** 徐州 **纬度:** 34.266666 **经度:** 117.166664 **查看:** 高德地图
www.douban.com	安全	是	**IP地址:** 140.143.177.206 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.tampermonkey.net	安全	否	**IP地址:** 46.4.58.236 **国家:** 德国 **地区:** 萨克森 **城市:** 法尔肯施泰因 **纬度:** 50.477852 **经度:** 12.371563 **查看:** Google 地图
ascii2d.net	安全	否	**IP地址:** 104.26.4.72 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

t.me	安全	否	**IP地址:** 104.26.4.72 **国家:** 大不列颠及北爱尔兰联合王国 **地区:** 英格兰 **城市:** 伦敦 **纬度:** 51.508530 **经度:** -0.125740 **查看:** Google 地图
www.so.com	安全	是	**IP地址:** 171.8.167.22 **国家:** 中国 **地区:** 河南 **城市:** 郑州 **纬度:** 34.757778 **经度:** 113.648613 **查看:** 高德地图
www.sohu.com	安全	是	**IP地址:** 18.232.30.203 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
www.cngwzj.com	安全	是	**IP地址:** 61.190.236.102 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
twitter.com	安全	否	**IP地址:** 67.63.62.131 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
search.yahoo.com	安全	否	**IP地址:** 67.63.62.131 **国家:** 美国 **地区:** 纽约 **城市:** 纽约市 **纬度:** 40.731323 **经度:** -73.990089 **查看:** Google 地图
www.sogou.com	安全	是	**IP地址:** 117.89.181.121 **国家:** 中国 **地区:** 江苏 **城市:** 南京 **纬度:** 32.061668 **经度:** 118.777992 **查看:** 高德地图
www.facebook.com	安全	否	**IP地址:** 149.56.28.34 **国家:** 加拿大 **地区:** 魁北克 **城市:** 蒙特利尔 **纬度:** 45.508839 **经度:** -73.587807 **查看:** Google 地图

metaso.cn	安全	是	**IP地址:** 49.7.37.75 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
m.weibo.cn	安全	是	**IP地址:** 49.7.37.75 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图
www.360doc.com	安全	是	**IP地址:** 49.7.36.23 **国家:** 中国 **地区:** 江苏 **城市:** 常州 **纬度:** 31.783331 **经度:** 119.966667 **查看:** 高德地图
startpage.com	安全	否	**IP地址:** 67.63.62.131 **国家:** 美国 **地区:** 弗吉尼亚州 **城市:** 阿什本 **纬度:** 39.039474 **经度:** -77.491806 **查看:** Google 地图
fastly.jsdelivr.net	安全	否	**IP地址:** 67.63.62.131 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.taodudu.cc	安全	是	**IP地址:** 38.238.213.56 **国家:** 中国 **地区:** 香港 **城市:** 香港 **纬度:** 22.285521 **经度:** 114.157692 **查看:** 高德地图
webtrans.yddao.com	安全	是	**IP地址:** 49.7.36.23 **国家:** 中国 **地区:** 贵州 **城市:** 遵义 **纬度:** 27.686441 **经度:** 106.907135 **查看:** 高德地图
card.weibo.com	安全	是	**IP地址:** 49.7.36.23 **国家:** 中国 **地区:** 北京 **城市:** 北京 **纬度:** 39.907501 **经度:** 116.397102 **查看:** 高德地图

google.com	安全	否	**IP地址:** 142.250.115.138 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 山景城 **纬度:** 37.405991 **经度:** -122.078514 **查看:** Google 地图
trace.moe	安全	否	**IP地址:** 104.25.244.47 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
saucenao.com	安全	否	**IP地址:** 104.26.15.28 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
www.ximalaya.com	安全	是	**IP地址:** 180.97.228.182 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.autohome.com.cn	安全	是	**IP地址:** 117.92.139.35 **国家:** 中国 **地区:** 江苏 **城市:** 连云港 **纬度:** 34.600025 **经度:** 119.166847 **查看:** 高德地图
www.giant.com.cn	安全	是	**IP地址:** 47.110.214.253 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
coolapk.com	安全	是	**IP地址:** 117.69.71.61 **国家:** 中国 **地区:** 安徽 **城市:** 苏州 **纬度:** 33.636440 **经度:** 116.978851 **查看:** 高德地图
www.qidian.com	安全	是	**IP地址:** 117.21.189.54 **国家:** 中国 **地区:** 江西 **城市:** 九江 **纬度:** 29.733330 **经度:** 115.983330 **查看:** 高德地图

www.taobao.com	安全	是	**IP地址:** 180.97.251.189 **国家:** 中国 **地区:** 江苏 **城市:** 苏州 **纬度:** 31.311365 **经度:** 120.617691 **查看:** 高德地图
www.thepaper.cn	安全	是	**IP地址:** 150.138.248.35 **国家:** 中国 **地区:** 山东 **城市:** 济南 **纬度:** 36.668331 **经度:** 116.997223 **查看:** 高德地图
app-measurement.com	安全	是	**IP地址:** 180.163.150.33 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
m.so.com	安全	是	**IP地址:** 180.163.251.63 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
www.bing.com	安全	否	**IP地址:** 23.198.7.180 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.783058 **经度:** -96.806503 **查看:** Google 地图
www.ithome.com	安全	是	**IP地址:** 27.221.82.35 **国家:** 中国 **地区:** 山东 **城市:** 青岛 **纬度:** 36.098610 **经度:** 120.371941 **查看:** 高德地图
my.cdn.com	安全	否	No Geolocation information available.
yz.m.sm.cn	安全	是	**IP地址:** 140.205.70.177 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图

duckduckgo.com	安全	否	**IP地址:** 40.89.244.232 **国家:** 美国 **地区:** 爱荷华州 **城市:** 得梅因 **纬度:** 41.600449 **经度:** -93.609116 **查看:** Google 地图
so.toutiao.com	安全	是	**IP地址:** 80.67.181.209 **国家:** 中国 **地区:** 江苏 **城市:** 镇江 **纬度:** 32.209366 **经度:** 119.434372 **查看:** 高德地图
viayoo.com	安全	是	**IP地址:** 47.98.219.161 **国家:** 中国 **地区:** 浙江 **城市:** 杭州 **纬度:** 30.293650 **经度:** 120.161583 **查看:** 高德地图
www.bilibili.com	安全	是	**IP地址:** 47.98.219.161 **国家:** 中国 **地区:** 浙江 **城市:** 金华 **纬度:** 30.013470 **经度:** 120.288658 **查看:** 高德地图
firebase-settings.crashlytics.com	安全	是	**IP地址:** 180.163.150.34 **国家:** 中国 **地区:** 上海 **城市:** 上海 **纬度:** 31.224333 **经度:** 121.468948 **查看:** 高德地图
easylist-downloads.adblockplus.org	安全	否	**IP地址:** 184.28.41.44 **国家:** 美国 **地区:** 得克萨斯州 **城市:** 达拉斯 **纬度:** 32.783058 **经度:** -96.806503 **查看:** Google 地图
tineye.com	安全	否	**IP地址:** 172.67.27.166 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图
3d.iqdb.org	安全	否	**IP地址:** 91.121.210.31 **国家:** 法国 **地区:** 上法兰西岛 **城市:** 鲁拜克斯 **纬度:** 50.693710 **经度:** 3.174439 **查看:** Google 地图

www.163.com	安全	是	**IP地址:** 221.230.244.113 **国家:** 中国 **地区:** 江苏 **城市:** 台州 **纬度:** 32.492168 **经度:** 119.910767 **查看:** 高德地图
res.viayoo.com	安全	否	**IP地址:** 104.21.16.1 **国家:** 美国 **地区:** 加利福尼亚 **城市:** 旧金山 **纬度:** 37.775700 **经度:** -122.395203 **查看:** Google 地图

URL链接分析

URL信息	源码文件
• https://dav.jianguoyun.com/dav/	i/a/m0/q/m.java
• https://translate.google.com/translate_a/element.js?cb=googletranslateelementinit	i/a/x/u/b.java
• www.10099.com.cn • https://wap.sogou.com/web/sl?keyword= • www.giant.com.cn • https://metaso.cn/search/3333?q=	i/a/x/n0/i0.java
• https://wap.sogou.com/web/sl?bid=sogou-mobb- • https://wap.sogou.com/web/sl?keyword= • https://www.sogou.com/web?query=	i/a/z/m/j.java
• https://metaso.cn/?q= • https://metaso.cn/?	i/a/z/m/g.java
• https://firebase.google.com/docs/crashlytics/get-started?platform=android#add-plugin	d/c/c/p/h/j/s.java
• https://startpage.com/do/search?query=	i/a/z/m/k.java
• https://pagead2.googlesyndication.com/pagead/gen_204?id=cmob-apps	d/c/a/b/a/a/b.java
• https://yz.m.sm.cn/s?q= • https://yz.m.sm.cn/s?from=	i/a/z/m/i.java
• https://api.bing.com/qsml.aspx?market=	i/a/z/q/j/b.java
• https://us.app.viayoo.com/api/user/? • https://us.app.viayoo.com/api/sync/ • https://us.app.viayoo.com/api/update • https://viayoo.com/en/docs/terms-of-use.html • https://viayoo.com/en/docs/privacy-policy.html	i/a/z/n/b.java
• https://viayoo.com/ • https://www.tampermonkey.net/documentation.php	i/a/e0/e1.java

• https://easylist-downloads.adblockplus.org/antiadblockfilters.txt • https://easylist-downloads.adblockplus.org/liste_ar.txt • https://easylist-downloads.adblockplus.org/koreanlist.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_13_turkish/filter.txt • https://easylist-downloads.adblockplus.org/latvianlist.txt • https://easylist-downloads.adblockplus.org/bulgarian_list.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_1_russian/filter.txt • https://easylist-downloads.adblockplus.org/abpvn.txt • https://easylist-downloads.adblockplus.org/easylistpolish.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_8_dutch/filter.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_16_french/filter.txt • https://easylist-downloads.adblockplus.org/rolist.txt • https://easylist-downloads.adblockplus.org/easylistlithuania.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_9_spanish/filter.txt • https://easylist-downloads.adblockplus.org/easylistitaly.txt • https://easylist-downloads.adblockplus.org/easylist.txt • https://easylist-downloads.adblockplus.org/israellist.txt • https://easylist-downloads.adblockplus.org/easyprivacy.txt • https://easylist-downloads.adblockplus.org/easylistchina.txt • https://easylist-downloads.adblockplus.org/abpindo.txt • https://easylist-downloads.adblockplus.org/indianlist.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_7_japanese/filter.txt • https://raw.githubusercontent.com/adguardteam/filtersregistry/master/filters/filter_6_german/filter.txt • https://fastly.jsdelivr.net/gh/cjx82630/cjxlist/cjx-annoyance.txt • https://easylist-downloads.adblockplus.org/easylistczechslovak.txt	d/g/c/d/c.java
• https://app.viayoo.com/api/sync? • https://app.viayoo.com/api/user? • https://viayoo.com/zh-cn/docs/privacy-policy.html • https://app.viayoo.com/api/update • https://viayoo.com/zh-cn/docs/terms-of-use.html	i/a/z/n/a.java
• https://sug.so.360.cn/suggest?encodein=utf-8&encodeout=utf-8&format=json&word=	i/a/z/q/j/d.java
• https://clients1.google.com/complete/search?hl=	i/a/z/q/j/c.java
• 127.0.0.1	d/g/c/c/d.java
• https://suggestion.baidu.com/su?wd=	i/a/z/q/j/a.java
• https://help.eyeo.com/en/adblockplus/how-to-write-filters	i/a/u/s0.java

• www.360doc.com/content/ • www.tofacebook.com • www.gushiwen.cn/* • www.360doc.com/content/* • www.360doc.cn/article/ • www.oschina.net/p/* • www.cn-healthcare.com/ • www.taodudu.cc/news/ • www.gushiwen.cn/ • www.ximalaya.com/ • www.cn-healthcare.com/* • www.zhihu.com/question • www.360doc.cn/article/* • www.tofacebook.com/* • www.zhihu.com/question/* • www.bilibili.com/read/mobile* • www.oschina.net/p/ • www.taodudu.cc/news/*	i/a/w/ea.java
• https://fastly.jsdelivr.net/npm/viewerjs@1.11.7/dist/viewer.min.css • https://fastly.jsdelivr.net/npm/viewerjs@1.11.7/dist/viewer.min.js	i/a/w/da.java
• https://viayoo.com/ • https://app.viayoo.com/addons/	i/a/z/p/e/d.java
• https://www.bing.com/search? • https://www.bing.com/search?q=	i/a/z/m/b.java
• https://m.so.com/s? • https://www.so.com/s?q= • https://m.so.com/s?q=	i/a/z/m/f.java
• http://viayoo.com/	i/a/v/c2.java
• https://m.baidu.com/s?from= • https://m.baidu.com/s?word= • https://www.baidu.com/s?ie=utf-8&from= • https://www.baidu.com/s?ie=utf-8&word=	i/a/z/m/a.java
• https://www.google.com/search? • https://www.google.com/search?q=	i/a/z/m/e.java
• https://www.google.com/search?q=	i/a/z/k/k.java
• https://goo.gl/naoooi	d/c/a/b/f/b/ua.java
• https://duckduckgo.com/?q=	i/a/z/m/d.java
• https://m.baidu.com/?tn=&from=1022560v • https://www.google.com/	i/a/x/u/a.java
• https://github.com/tuyafeng/via • http://viayoo.com/contact/qqgroup/ • http://viayoo.com/ • https://t.me/viatg	i/a/z/j/d.java
• https://%s/%s/%s	d/c/c/v/n/c.java
• https://firebase.google.com/docs/analytics	d/c/a/b/e/c/s2.java
• https://fastly.jsdelivr.net/npm/viewerjs@1.11.7/dist/viewer.min.css • https://fastly.jsdelivr.net/npm/viewerjs@1.11.7/dist/viewer.min.js	i/a/z/j/c.java

• https://firebase.google.com/support/privacy/init-options	d/c/c/v/f.java
• https://firebase.google.com/support/guides/disable-analytics	d/c/a/b/f/b/m3.java
• www.huanqiu.com • https://hanyu.baidu.com/s?wd= • https://hanyu.baidu.com/hanyu-page/term/detail?wd= • https://tieba.baidu.com/f?ie=utf-8&kw= • https://wenku.baidu.com/search?word= • https://m.weibo.cn/ • www.hao123.com • https://hanyu.baidu.com/zici/s?wd= • www.jd.com • https://weibo.com/ttarticle/p/show?id= • www.xs8.cn • https://pan.baidu.com/wap/home#/dir/ • https://m.weibo.cn/detail/ • www.sohu.com/a/ • https://weibo.com/0/ • www.cngwzj.com/ • www.guoxuedashi.net • https://zhidao.baidu.com/search?ie=utf-8&word= • www.ccopyright.com.cn/mobile/ • www.ithome.com/0/ • https://card.weibo.com/article/m/show/id/ • www.autohome.com.cn • www.hupu.com/ • www.guancha.cn • https://pan.baidu.com/wap/home#/ • https://image.baidu.com/search/index?tn=baiduimage&ie=utf-8&word= • www.so.com • https://pan.baidu.com/disk/main#/index?category=all&path= • https://pan.baidu.com/disk/main#/index?category=all • www.ccopyright.com.cn/ • www.qidian.com • www.taobao.com • www.ithome.com/ • https://hanyu.baidu.com/hanyu-page/zici/s?wd= • www.thepaper.cn • www.douban.com/people/ • www.163.com • www.baidu.com	i/a/x/h0/o0.java
• https://yandex.com/search/?text= • https://yandex.com/search/touch/?text=	i/a/z/m/n.java
• https://search.yahoo.com/search?p= • https://search.yahoo.com/search?	i/a/z/m/m.java
• https://so.toutiao.com/search?keyword= • https://so.toutiao.com/search?	i/a/z/m/l.java
• https://app-measurement.com/a	d/c/a/b/f/b/i3.java
• https://www.google.com • www.google.com	d/c/a/b/f/b/n7.java
• https://app-measurement.com/a	d/c/a/b/e/c/fc.java
• javascript:try{opensuggestion.pushsuggestions • http://vidyoo.com/	i/a/w/x9.java
• https://file-examples.com/wp-content/uploads/2017/04/file_example_mp4_480_1_5mg.mp4	i/a/k0/j6.java

• https://www.google.com/search?q=	i/a/x/h0/j1.java
• https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings	d/c/c/p/h/p/e.java
• https://wormhole.app/download-stream/ • http://webtrans.yodao.com/webtranspc/index.html#/?url= • https://saucenao.com/search.php?db=999&url= • https://3d.iqdb.org/?url= • https://graph.baidu.com/details?isfromtusoupc=1&tn=pc&carousel=0&promotion_name=pc_image_shituindex&extuidata%5bislogoshow%5d=1&image= • https://www.bing.com/images/search?view=detailv2&iss=sbi&form=sbivsp&sbisrc=urlpaste&q=imgurl: • https://fanyi.baidu.com/transpage?query= • https://app.viayoo.com/addons/ • https://translate.google.com/translate?sl=auto&tl= • https://st.so.com/r?img_url= • https://trace.moe/?url= • https://ascii2d.net/search/url/ • https://iqdb.org/?url= • https://yandex.com/images/touch/search?family=yes&rpt=imageview&url= • https://tineye.com/search/?url= • https://lens.google.com/uploadbyurl?url=	i/a/w/u9.java
• 127.0.0.1	i/a/k0/s6.java
• https://github.com/promeg/tinypinyin • https://github.com/shwenzhang/AndResGuard • https://github.com/uber/autodispose • https://github.com/thegrizzlylabs/sardine-android • https://github.com/rburgst/okhttp-digest • https://github.com/fengyuanchen/viewerjs • https://github.com/jaredsburrows/userscript • https://github.com/aflorestad/drag-select-recyclerview • https://github.com/androidx/androidx • https://github.com/jakewharton/timber	i/a/k0/n6.java
• javascript:try{window.__setmarkerenabled	i/a/w/q9.java
• http://viayoo.com/contact/uggroup/ • https://github.com/tuyafeng/Via • http://viayoo.com/contact/telegram-zh/ • https://weibo.com/u/7558014976 • https://beian.miit.gov.cn/ • https://twitter.com/tuyafeng • http://viayoo.com/contact/wechat/ • https://support.qq.com/product/438363 • http://viayoo.com/contact/telegram/	i/a/k0/a6.java
• https://google.com/search?	d/c/a/b/f/b/m7.java

本报告由南明离火移动安全分析平台生成

• http://coolapk.com/apk/ • https://play.google.com/store/apps/details?id=	i/a/x/h0/d0.java
• https://res.viayoo.com/v1/latest_cn.json • https://res.viayoo.com/v1/latest_play.json	i/a/x/g0/i.java
• https://lingva.retiolus.net/api/v1/	i/a/z/s/a.java
• https://c.viayoo.com/api/frontend • https://us-c.viayoo.com/api/frontend	i/a/z/h/f.java
• https://www.google.com/any/not_me • https://www.google.com/any/* • https://www.google.com/something • https://my.cdn.com/jquery.js	自研引擎-S

第三方SDK

SDK名称	开发者	描述信息
File Provider	Android	FileProvider 是 ContentProvider 的特殊子类，它通过创建 content://Uri 代替 file:///Uri 以促进安全分享与应用程序关联的文件。
Firebase	Google	Firebase 提供了分析、数据库、消息传递和崩溃报告等功能，可助您快速采取行动并专注于您的用户。
Firebase Analytics	Google	Google Analytics（分析）是一款免费的应用衡量解决方案，可提供关于应用使用情况和用户互动度的分析数据。

邮箱

EMAIL	源码文件
wiar1824@gmail.com 2376688759@qq.com	i/a/z/j/d.java
yafengtu@gmail.com	i/a/k0/e6.java
yafengtu@gmail.com	i/a/k0/a6.java
wiar1824@gmail.com 2376688759@qq.com	自研引擎-S

追踪器

名称	类别	网址
Google CrashLytics	Crash reporting	https://reports.exodus-privacy.eu.org/trackers/27
Google Firebase Analytics	Analytics	https://reports.exodus-privacy.eu.org/trackers/49

密钥凭证

可能的密钥

"com.google.firebase.crashlytics.mapping_file_id" : "none"
"google_app_id" : "1:1029963211769:android:b26731d70ba09c4fce5328"
5ae8018a613c7b4ef6297b23aaf7d5d18d16cac9a6636ae20d378aa2
fa6f3153b591e06fbf0170d935ad0afe
470fa2b4ae81cd56ecbcda9735803434cec591fa

免责声明及风险提示: