MoGua

搜磁器 1.2.4.APK 分析报告

APP名称:	搜磁器
包名:	com.somagnet
域名线索:	45条
URL线索:	21条
邮箱线索:	0条

分析日期:	2025年1月9日
分析平台:	摸瓜APK反编译平台

文件信息

文件名: 搜磁器_1.2.4.apk
文件大小: 7.59MB
MD5值: 60e47e382f3b0c645a3acf77c1594a3c
SHA1值: 646875d6f1183ea2e60f176ab86d7f74efb58f7e
SHA256值: a2d8a8dee26e6e34e72baa031fbd463132b48010343a619de57ce8f116a4a290

APP 信息

App名称: 搜磁器
包名: com.somagnet
主活动Activity: com.one.somagnet.ui.activity.LauncherActivity
安卓版本名称: 1.2.4
安卓版本: 25

域名线索

域名	服务器信息

px-intl.ucweb.com	**IP**: 157.185.188.1 **所属国家**: Canada **地区**: Ontario **城市**: North York **纬度**: 43.771862 **经度**: -79.331528
errlogos.umeng.com	**IP**: 47.246.110.96 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
h.trace.qq.com	**IP**: 113.56.189.246 **所属国家**: China **地区**: Hubei **城市**: Huangshi **纬度**: 30.204170 **经度**: 115.077606
schemas.android.com	没有服务器地理信息.
w3.org	**IP**: 104.18.23.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
alogsus.umeng.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
aaid.umeng.com	**IP**: 223.109.148.171 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
www.cltt667.buzz	**IP**: 91.195.240.12 **所属国家**: Germany **地区**: Nordrhein-Westfalen **城市**: Koeln **纬度**: 50.933346 **经度**: 6.949720
	IP: 124.95.225.169 **所属国家**: China

android.bugly.qq.com	**地区**: Liaoning **城市**: Shenyang **纬度**: 41.792221 **经度**: 123.432877
zhongzilou.com	IP: 157.240.8.50 **所属国家**: Australia **地区**: New South Wales **城市**: Sydney **纬度**: -33.867779 **经度**: 151.207047
7m0vfwt.xyz	IP: 31.13.69.169 **所属国家**: Ireland **地区**: Dublin **城市**: Dublin **纬度**: 53.344151 **经度**: -6.267249
zzb03.cfd	IP: 45.142.157.26 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.604309 **经度**: -122.329842
xccl89.xyz	IP: 104.21.34.141 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.btmulu.pw	IP: 172.67.128.100 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
00mag.sbs	IP: 45.142.157.26 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.604309 **经度**: -122.329842
thepiratebay10.xyz	IP: 172.67.184.161 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

dmhy.anoneko.com	**IP**: 128.121.243.228 **所属国家**: United States of America **地区**: Washington **城市**: Redmond **纬度**: 47.682899 **经度**: -122.120903
ouplog.umeng.com	**IP**: 47.246.110.93 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
doc2.htmcdn.com	**IP**: 38.199.108.55 **所属国家**: United States of America **地区**: District of Columbia **城市**: Washington **纬度**: 38.901566 **经度**: -77.050781
so.acg17.cc	**IP**: 172.67.209.10 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
hhsbd02.towercloud.world	**IP**: 8.223.113.59 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
alogus.umeng.com	**IP**: 223.109.148.141 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
developer.umeng.com	**IP**: 59.82.29.162 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
	IP: 119.28.121.133 **所属国家**: Singapore **地区**: Singapore

astat.bugly.qcloud.com	**城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
www.w3.org	IP: 104.18.22.19 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.torrentkitty.ink	IP: 172.67.201.184 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
plbslog.umeng.com	IP: 36.156.202.68 **所属国家**: China **地区**: Jiangsu **城市**: Yangzhou **纬度**: 32.397221 **经度**: 119.435600
xml.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
px.ucweb.com	IP: 116.132.217.40 **所属国家**: China **地区**: Hebei **城市**: Shijiazhuang **纬度**: 38.041599 **经度**: 114.478081
astat.bugly.cros.wr.pvp.net	IP: 170.106.118.26 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.774929 **经度**: -122.419418
wuqianyu.top	IP: 64.64.227.109 **所属国家**: United States of America **地区**: California **城市**: Los Angeles **纬度**: 34.052986 **经度**: -118.263687

clhztop-666971be0d3df.towercloud.world	**IP**: 8.223.113.59 **所属国家**: Singapore **地区**: Singapore **城市**: Singapore **纬度**: 1.289987 **经度**: 103.850281
ulogs.umengcloud.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
errlog.umeng.com	**IP**: 223.109.148.129 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
sobt12.top	**IP**: 45.151.132.102 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.620621 **经度**: -122.310959
clg38.sbs	**IP**: 45.142.157.26 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.604309 **经度**: -122.329842
clm41.icu	**IP**: 45.151.132.102 **所属国家**: United States of America **地区**: Washington **城市**: Seattle **纬度**: 47.620621 **经度**: -122.310959
btsao.com	**IP**: 108.160.162.31 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
btfox19.top	**IP**: 45.142.157.26 **所属国家**: United States of America **地区**: Washington

	城市: Seattle **纬度**: 47.604309 **经度**: -122.329842
ulogs.umeng.com	**IP**: 223.109.148.178 **所属国家**: China **地区**: Jiangsu **城市**: Nanjing **纬度**: 32.061668 **经度**: 118.777992
xccl94.xyz	**IP**: 172.67.221.159 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
www.sokk34.buzz	**IP**: 199.59.149.207 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.773968 **经度**: -122.410446
vbinupmk.1024194.xyz	**IP**: 172.67.193.189 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203
pslog.umeng.com	**IP**: 59.82.60.43 **所属国家**: China **地区**: Zhejiang **城市**: Hangzhou **纬度**: 30.293650 **经度**: 120.161583
clp108.shop	**IP**: 104.21.36.21 **所属国家**: United States of America **地区**: California **城市**: San Francisco **纬度**: 37.775700 **经度**: -122.395203

URL线索

URL**信息**	Url**所在文件**

https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/f/c.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/efs/sdk/base/core/controller/ControllerCenter.java
http://xml.apache.org/xslt	com/blankj/utilcode/util/LogUtils.java
http://schemas.android.com/apk/res/android	com/hjq/permissions/i.java
https://h.trace.qq.com/kv	com/tencent/bugly/proguard/r.java
https://android.bugly.qq.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/StrategyBean.java
https://astat.bugly.qcloud.com/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://astat.bugly.cros.wr.pvp.net/:8180/rqd/async	com/tencent/bugly/crashreport/common/strategy/a.java
https://errlogos.umeng.com/upload	com/uc/crashsdk/e.java
https://errlog.umeng.com/upload	com/uc/crashsdk/e.java
https://errlogos.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://errlog.umeng.com/api/crashsdk/logcollect	com/uc/crashsdk/a/h.java
https://px-intl.ucweb.com	com/uc/crashsdk/a/h.java
https://px.ucweb.com	com/uc/crashsdk/a/h.java
https://errlogos.umeng.com	com/uc/crashsdk/a/d.java
https://errlog.umeng.com	com/uc/crashsdk/a/d.java
http://developer.umeng.com/docs/66650/cate/66650	com/umeng/analytics/pro/j.java
https://developer.umeng.com/docs/66632/detail/	com/umeng/commonsdk/debug/UMLogUtils.java
https://developer.umeng.com/docs/119267/detail/182050	com/umeng/commonsdk/debug/UMLogCommon.java
https://plbslog.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ulogs.umeng.com	com/umeng/commonsdk/stateless/a.java
https://ouplog.umeng.com	com/umeng/commonsdk/stateless/a.java

https://ulogs.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://alogsus.umeng.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://ulogs.umengcloud.com	com/umeng/commonsdk/statistics/UMServerURL.java
https://pslog.umeng.com	com/umeng/commonsdk/vchannel/a.java
https://pslog.umeng.com/	com/umeng/commonsdk/vchannel/a.java
https://aaid.umeng.com/api/updateZdata	com/umeng/umzid/ZIDManager.java
https://aaid.umeng.com/api/postZdata	com/umeng/umzid/ZIDManager.java
http://w3.org/1999/xhtml	org/htmlcleaner/x.java
http://sobt12.top	摸瓜V2引擎
http://sobt12.top/[keyword].html?sort\u003drel\u0026page\u003d[page]	摸瓜V2引擎
http://sobt12.top/q/%E7%BE%8E%E5%A5%B3.html	摸瓜V2引擎
https://hhsbd02.towercloud.world/	摸瓜V2引擎
https://hhsbd02.towercloud.world/boss_search.php?keywords\u003d[keyword]\u0026page\u003d[page]\u0026action\u003d1	摸瓜V2引擎
https://hhsbd02.towercloud.world	摸瓜V2引擎
http://sobt12.top/[keyword]?sort\u003drel\u0026page\u003d[page]	摸瓜V2引擎
http://sobt12.top/s/%E7%BE%8E%E5%A5%B3.html	摸瓜V2引擎
https://clm41.icu/kw	摸瓜V2引擎
https://clm41.icu/[keyword]\u0026sort\u003drele\u0026p\u003d[page]	摸瓜V2引擎
https://clm41.icu/search?word\u003d%E7%BE%8E%E5%A5%B3	摸瓜V2引擎
http://clg38.sbs/	摸瓜V2引擎
http://clg38.sbs/[keyword]\u0026sort\u003drele\u0026p\u003d[page]	摸瓜V2引擎
http://clg38.sbs/search?word\u003d%E7%BE%8E%E5%A5%B3	摸瓜V2引擎
http://btfox19.top/	摸瓜V2引擎

http://btfox19.top/[keyword]\u0026sort\u003dtime\u0026page\u003d[page]	摸瓜V2引擎
http://btfox19.top	摸瓜V2引擎
http://00mag.sbs	摸瓜V2引擎
http://00mag.sbs/[keyword]\u0026p\u003d[page]	摸瓜V2引擎
http://zzb03.cfd/	摸瓜V2引擎
http://zzb03.cfd/[keyword]\u0026sort\u003drel\u0026page\u003d[page]	摸瓜V2引擎
http://zzb03.cfd	摸瓜V2引擎
https://vbinupmk.1024194.xyz	摸瓜V2引擎
https://vbinupmk.1024194.xyz/main-search-kw-[keyword]-[page].html	摸瓜V2引擎
https://www.sokk34.buzz/	摸瓜V2引擎
https://www.sokk34.buzz/search/[keyword]/page-[page].html	摸瓜V2引擎
https://7m0vfwt.xyz	摸瓜V2引擎
https://7m0vfwt.xyz/search-[keyword]-0-0-[page].html	摸瓜V2引擎
https://xccl94.xyz	摸瓜V2引擎
https://xccl94.xyz/search/kw-[keyword]-[page].html	摸瓜V2引擎
https://www.btmulu.pw/	摸瓜V2引擎
https://www.btmulu.pw/search/[keyword]/page-[page].html	摸瓜V2引擎
https://so.acg17.cc/	摸瓜V2引擎
https://so.acg17.cc/search-[keyword].htm	摸瓜V2引擎
https://www.torrentkitty.ink/search/[keyword]/[page]	摸瓜V2引擎
https://www.torrentkitty.ink/	摸瓜V2引擎
https://www.torrentkitty.ink/search/%E5%A4%8D%E4%BB%87%E8%80%85%E8%81%94%E7%9B%9F/1? __cf_chl_tk\u003dKyxtLv2hp5trtWHu1Fl0d5Ck7uX0HKDirblH4Q4kxJw-1642768927-0-gaNycGzNB-U	摸瓜V2引擎

https://wuqianyu.top/	摸瓜V2引擎
https://wuqianyu.top/search?keyword\u003d[keyword]\u0026sos\u003drelevance\u0026sofs\u003dall\u0026sot\u003dall\u0026soft\u003dall\u0026som\u003dexact\u0026p\u003d[page]	摸瓜V2引擎
https://wuqianyu.top	摸瓜V2引擎
https://zhongzilou.com/	摸瓜V2引擎
https://zhongzilou.com/list/[keyword]/[page]	摸瓜V2引擎
https://clp108.shop/	摸瓜V2引擎
https://clp108.shop/Search/[keyword]?page\u003d[page]	摸瓜V2引擎
https://clp108.shop	摸瓜V2引擎
https://btsao.com	摸瓜V2引擎
https://btsao.com/zh-cn/search/[keyword]/[page]?c\u003d\u0026s\u003dcreate_time	摸瓜V2引擎
https://clhztop-666971be0d3df.towercloud.world	摸瓜V2引擎
https://clhztop-666971be0d3df.towercloud.world/search_plus.php?keywords\u003d[keyword]\u0026page\u003d[page]\u0026action\u003d1	摸瓜V2引擎
https://xccl89.xyz	摸瓜V2引擎
https://xccl89.xyz/search/kw-[keyword]-[page].html	摸瓜V2引擎
https://dmhy.anoneko.com/	摸瓜V2引擎
https://dmhy.anoneko.com/topics/list/page/[page]?keyword\u003d[keyword]	摸瓜V2引擎
https://www.cltt667.buzz/	摸瓜V2引擎
https://www.cltt667.buzz/search-[keyword]-1-2-[page].html	摸瓜V2引擎
https://thepiratebay10.xyz/	摸瓜V2引擎
https://thepiratebay10.xyz/search/[keyword]/[page]/99/0	摸瓜V2引擎
https://doc2.htmcdn.com:39988/	摸瓜V2引擎
https://doc2.htmcdn.com:39988/search?word\u003d[keyword]\u0026sort\u003d\u0026page\u003d[page]	摸瓜V2引擎
https://doc2.htmcdn.com:39988/search?word\u003d%E7%BE%8E%E5%A5%B3	摸瓜V2引擎

https://errlog.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com/api/crashsdk/logcollect	lib/armeabi-v7a/libcrashsdk.so
https://errlog.umeng.com	lib/armeabi-v7a/libcrashsdk.so
https://errlogos.umeng.com	lib/armeabi-v7a/libcrashsdk.so
http://www.	lib/armeabi-v7a/libnmmp.so

邮箱线索

手机线索

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=CN, ST=JiangXi, L=NanChang, O=somagnet, OU=somagnet, CN=Siyu
签名算法: rsassa_pkcs1v15
有效期自: 2021-05-16 03:15:53+00:00
有效期至: 2103-07-06 03:15:53+00:00
发行人: C=CN, ST=JiangXi, L=NanChang, O=somagnet, OU=somagnet, CN=Siyu
序列号: 0x24fe2090
哈希算法: sha1
md5值: 979327fbac79674ea05603d2d814f29f
sha1值: 30a40dbd76902066314e2e291778a52621a989ce
sha256值: 8ac3ffc98708e88660031e4135c48d37e055f4d38b35d3f4b859143b87eeabf3
sha512值: 74fd5570895db77ab065290216917e6835bb82b0af6047ecc45563b073728b14c371c7c4605d073bba046870f2dd609457e09ede7c671f560546272ace816f3a
公钥算法: rsa
密钥长度: 2048
指纹: 5682fcd8040b007fd27bd3687e97aa62e9597d2ba5d42d4f93f4b4419a97a457

硬编码敏感信息

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.INTERNET	正常	互联网接入	允许应用程序创建网络套接字
android.permission.RECORD_AUDIO	危险	录音	允许应用程序访问音频记录路径
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.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.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.READ_CONTACTS	危险	读取联系人数据	允许应用程序读取您手机上存储的所有联系人（地址）数据。恶意应用程序可以借此将您的数据发送给其他人
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.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.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.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.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.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.MOUNT_UNMOUNT_FILESYSTEMS	危险	装载和卸载文件系统	允许应用程序为可移动存储安装和卸载文件系统

应用内通信