Evaluation Warning: The document was created with Spire.Doc for Python.

**AdGuard（ 4.11.7版本）   
APK分析报告**

## **1. 分析结果概述**

**说明：本分析结果由摸瓜网站自动生成，一共包含以下10类内容：（1）分析结果概述（2）APK文件基本信息（3）APP基本信息（4）线索情况（5）签名证书（6）硬编码敏感信息（7）加壳分析（8）第三方插件（9）此APP的危险动作（10）应用内通信。  
\*此分析结果仅供参考，请勿商用。\*。**

| 类别 | 内容 |
| --- | --- |
| APP名称 | AdGuard |
| 版本 | 4.11.7 |
| 包名 | com.adguard.android |
| 域名线索 | 61条 |
| URL线索 | 39条 |
| APP图标 |  |
| 分析日期 | 2025年6月19日 |
| 分析平台 | [摸瓜APK反编译平台](https://mogua.co) |

## **2. APK文件基本信息**

| 类别 | 内容 |
| --- | --- |
| 文件名 | Adguard\_v4.11.7\_MOD.apk |
| 文件大小 | 66.23MB |
| MD5值 | 458da89ac1eb8d3efa48b2f166dc662b |
| SHA1值 | 0cb16418dbecb3457003b30fd50b9963756f088c |
| SHA256值 | e8946f49cb368f2a794952cca306b505257ea6304edbb51053ac58a6eee423e3 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | AdGuard |
| 包名 | com.adguard.android |
| 主活动Activity | com.adguard.android.ui.activity.SplashActivity |
| 安卓版本名称 | 4.11.7 |
| 安卓版本 | 10282090 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| malware-filter.gitlab.io | IP: 35.185.44.232  所属国家: United States of America  地区: South Carolina  城市: North Charleston |
| link.adtidy.org | IP: 104.18.25.57  所属国家: United States of America  地区: California  城市: San Francisco |
| www.fanboy.co.nz | IP: 172.67.73.29  所属国家: United States of America  地区: California  城市: San Francisco |
| gitlab.com | IP: 172.65.251.78  所属国家: United States of America  地区: California  城市: San Francisco |
| mobile-api.adguard.org | IP: 172.67.70.82  所属国家: United States of America  地区: California  城市: San Francisco |
| xml.org | IP: 104.239.142.8  所属国家: United States of America  地区: Texas  城市: Windcrest |
| youtu.be | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| www.zoso.ro | IP: 104.21.32.1  所属国家: United States of America  地区: California  城市: San Francisco |
| apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| zoso.ro | IP: 104.21.64.1  所属国家: United States of America  地区: California  城市: San Francisco |
| fanboy.co.nz | IP: 172.67.73.29  所属国家: United States of America  地区: California  城市: San Francisco |
| stanev.org | IP: 172.67.196.239  所属国家: United States of America  地区: California  城市: San Francisco |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| raw.githubusercontent.com | IP: 185.199.110.133  所属国家: United States of America  地区: Pennsylvania  城市: California |
| www.baidu.com | IP: 110.242.69.21  所属国家: China  地区: Hebei  城市: Baoding |
| family.adguard-dns.com | IP: 94.140.15.16  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| logback.qos.ch | IP: 159.100.250.151  所属国家: Switzerland  地区: Zurich  城市: Zurich |
| dns.adguard-dns.com | IP: 94.140.15.15  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| filters.adtidy.org | IP: 143.244.51.52  所属国家: United States of America  地区: California  城市: Los Angeles |
| list-kr.github.io | IP: 185.199.111.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| youtube.com | IP: 31.13.94.36  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| example.org | IP: 96.7.128.186  所属国家: United States of America  地区: California  城市: El Segundo |
| adblock.gardar.net | IP: 82.221.78.5  所属国家: Iceland  地区: Hofudborgarsvaedi  城市: Reykjavik |
| api.adguard.org | IP: 104.26.13.10  所属国家: United States of America  地区: California  城市: San Francisco |
| www.void.gr | IP: 83.212.168.30  所属国家: Greece  地区: Attiki  城市: Athens |
| forums.lanik.us | IP: 172.67.134.228  所属国家: United States of America  地区: California  城市: San Francisco |
| hg.adblockplus.org | IP: 34.36.168.233  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| easylist-downloads.adblockplus.org | IP: 23.216.153.71  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| api.agrd-tm.com | IP: 172.67.151.61  所属国家: United States of America  地区: California  城市: San Francisco |
| play.google.com | IP: 8.7.198.46  所属国家: United States of America  地区: Louisiana  城市: Monroe |
| auth.adguard.org | IP: 104.26.12.10  所属国家: United States of America  地区: California  城市: San Francisco |
| icons.adguard.org | IP: 172.67.70.82  所属国家: United States of America  地区: California  城市: San Francisco |
| secure.fanboy.co.nz | IP: 104.26.15.96  所属国家: United States of America  地区: California  城市: San Francisco |
| abpvn.com | IP: 172.67.171.21  所属国家: United States of America  地区: California  城市: San Francisco |
| dns.adguard.com | IP: 94.140.14.14  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| www.bing.com | IP: 202.89.233.101  所属国家: China  地区: Beijing  城市: Beijing |
| duckduckgo.com | IP: 107.181.166.244  所属国家: United States of America  地区: California  城市: San Francisco |
| unfiltered.adguard-dns.com | IP: 94.140.14.140  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| dns-unfiltered.adguard.com | IP: 94.140.14.141  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| alleblock.pl | IP: 77.79.227.242  所属国家: Poland  地区: Mazowieckie  城市: Warsaw |
| polishannoyancefilters.netlify.app | IP: 52.76.120.174  所属国家: Singapore  地区: Singapore  城市: Singapore |
| easylist.to | IP: 104.21.60.31  所属国家: United States of America  地区: California  城市: San Francisco |
| adblock.ee | IP: 51.255.198.110  所属国家: France  地区: Hauts-de-France  城市: Roubaix |
| www.youtube.com | IP: 142.251.215.238  所属国家: United States of America  地区: California  城市: Mountain View |
| search.yahoo.com | IP: 88.191.249.183  所属国家: France  地区: Ile-de-France  城市: Paris |
| www.w3.org | IP: 104.18.22.19  所属国家: United States of America  地区: California  城市: San Francisco |
| xfiles.noads.it | IP: 86.107.32.84  所属国家: Italy  地区: Lazio  城市: Fonte Nuova |
| google.com | IP: 59.24.3.174  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| userscripts.adtidy.org | IP: 89.187.187.15  所属国家: United States of America  地区: California  城市: Los Angeles |
| pgl.yoyo.org | IP: 213.230.210.230  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Brighouse |
| www.i-dont-care-about-cookies.eu | IP: 54.148.2.18  所属国家: United States of America  地区: Oregon  城市: Boardman |
| m.youtube.com | IP: 199.59.148.96  所属国家: United States of America  地区: California  城市: San Francisco |
| abpchina.org | IP: 64.190.63.222  所属国家: Germany  地区: Nordrhein-Westfalen  城市: Koeln |
| kb.adguard.com | IP: 104.18.164.229  所属国家: United States of America  地区: California  城市: San Francisco |
| f-droid.org | IP: 192.133.77.197  所属国家: United States of America  地区: California  城市: San Francisco |
| www.google.com | IP: 31.13.94.37  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.slf4j.org | IP: 195.15.222.169  所属国家: Switzerland  地区: Geneve  城市: Carouge |
| dns-family.adguard.com | IP: 94.140.14.15  所属国家: Cyprus  地区: Lemesos  城市: Limassol |
| yandex.com | IP: 5.255.255.77  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| yandex.ru | IP: 77.88.55.88  所属国家: Russian Federation  地区: Moskva  城市: Moscow |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://filters.adtidy.org/android/filters\_i18n.js | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=filter\_policy&from=filter\_consent | C2/b.java |
| https://filters.adtidy.org/android/filters/ | C2/b.java |
| https://filters.adtidy.org/android/filters.js | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=faq\_filters&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=kb\_firefox\_certificates | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=global\_privacy\_control&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=how-does-adguard-protection-work | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=kb\_https\_filtering | C2/b.java |
| https://icons.adguard.org/icon | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=licenses | C2/b.java |
| https://api.adguard.org/account/api/1.0/products/licenses/application.json?app\_name= | C2/b.java |
| https://auth.adguard.org/api/1.0/user\_lookup | C2/b.java |
| https://auth.adguard.org/oauth/authorize? | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=privacy&from=license\_promo | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=privacy&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=background\_work&from=support | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=recovery\_password&from=license\_activation | C2/b.java |
| https://auth.adguard.org/api/1.0/registration?appVersion=4.11.7 | C2/b.java |
| https://link.adtidy.org/forward.html?&action=report | C2/b.java |
| https://mobile-api.adguard.org/api/1.0/requesttrial.html?app\_name= | C2/b.java |
| https://mobile-api.adguard.org/api/1.0/resetlicense.html?app\_name= | C2/b.java |
| https://auth.adguard.org/api/2.0/reset\_password | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=kb\_samsung\_pay\_ko | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=outbound\_proxy&from=info | C2/b.java |
| https://mobile-api.adguard.org/api/1.0/status.html?key=4DDBE80A3DA94D819A00523252FB6380&app\_name= | C2/b.java |
| https://api.adguard.org/account/api/1.0/account/info | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=stealth\_mode&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=account&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=support | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=acknowledgments&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=kb\_automation&from=automation | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=adguard\_cert\_module&from= | C2/b.java |
| https://api.agrd-tm.com/api/v1/event | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=download\_adguard&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=faq\_not\_support\_browsers | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=download\_adguard\_vpn&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=versionhistory&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=adguard\_vpn\_homepage&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=home&from=license\_activation | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=faq\_apps\_conflicts | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=whats-new-release-notes-in-blog&from= | C2/b.java |
| https://auth.adguard.org/oauth/token | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=battery\_info&from=battery\_usage\_screen | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=browsing\_security&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=purchase&from=license\_purchase&license\_key= | C2/b.java |
| https://mobile-api.adguard.org/api/2.0/checkupdate.html?app\_name= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=create\_your\_own\_filters&from=filters | C2/b.java |
| https://auth.adguard.org/oauth/device\_authorization | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=dns\_filtering&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=dns\_filtering\_syntax&from=filters | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=kb\_dns\_providers&from=dns\_servers\_list | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=do\_not\_track&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=eula&from=license\_promo | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=eula&from= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=userscripts&from=userscripts | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=faq&from=support | C2/b.java |
| https://mobile-api.adguard.org/api/2.0/feedback.html?key=4DDBE80A3DA94D819A00523252FB6380&app\_name= | C2/b.java |
| https://link.adtidy.org/forward.html?app=android&v=4.11.7&action=filter\_lists&from= | C2/b.java |
| https://github.com/ReactiveX/RxJava/wiki/Plugins | P5/d.java |
| https://github.com/ReactiveX/RxJava/wiki/Error-Handling | R5/d.java |
| https://github.com/ReactiveX/RxJava/wiki/What's-different-in-2.0 | R5/f.java |
| http://example.org | Y0/c.java |
| https://www.baidu.com/s?wd= | Y1/c.java |
| https://www.bing.com/search?q= | Y1/c.java |
| https://www.google.com/search?q= | Y1/c.java |
| https://yandex.com/?q= | Y1/c.java |
| https://search.yahoo.com/search?p= | Y1/c.java |
| https://duckduckgo.com/?q= | Y1/c.java |
| https://www.baidu.com/sugrec?json=1&prod=pc&wd= | Y1/c.java |
| https://www.bing.com/AS/Suggestions?qry= | Y1/c.java |
| https://google.com/complete/search?client=chrome&q= | Y1/c.java |
| https://yandex.ru/suggest/suggest-ya.cgi?v=4&n=10&part= | Y1/c.java |
| https://search.yahoo.com/sugg/gossip/gossip-us-ura/?output=fxjson&command= | Y1/c.java |
| https://duckduckgo.com/ac/?q= | Y1/c.java |
| https://easylist.to/\ | M/C2743a.java |
| https://secure.fanboy.co.nz/easylist.txt\ | M/C2743a.java |
| https://github.com/ABPindo/indonesianadblockrules\ | M/C2743a.java |
| https://raw.githubusercontent.com/ABPindo/indonesianadblockrules/master/subscriptions/abpindo.txt\ | M/C2743a.java |
| https://stanev.org/abp/\ | M/C2743a.java |
| https://stanev.org/abp/adblock\_bg.txt\ | M/C2743a.java |
| https://github.com/easylist/easylistchina\ | M/C2743a.java |
| https://raw.githubusercontent.com/easylist/easylistchina/master/easylistchina.txt\ | M/C2743a.java |
| https://github.com/tomasko126/easylistczechandslovak\ | M/C2743a.java |
| https://raw.githubusercontent.com/tomasko126/easylistczechandslovak/master/filters.txt\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/easylistdutch.txt\ | M/C2743a.java |
| https://easylist.to/easylistgermany/easylistgermany.txt\ | M/C2743a.java |
| https://github.com/easylist/EasyListHebrew\ | M/C2743a.java |
| https://raw.githubusercontent.com/easylist/EasyListHebrew/master/EasyListHebrew.txt\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/easylistitaly.txt\ | M/C2743a.java |
| https://github.com/EasyList-Lithuania/easylist\_lithuania\ | M/C2743a.java |
| https://raw.githubusercontent.com/EasyList-Lithuania/easylist\_lithuania/master/easylistlithuania.txt\ | M/C2743a.java |
| https://github.com/Latvian-List/adblock-latvian\ | M/C2743a.java |
| https://raw.githubusercontent.com/Latvian-List/adblock-latvian/master/lists/latvian-list.txt\ | M/C2743a.java |
| https://forums.lanik.us/viewforum.php?f=98\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/Liste\_AR.txt\ | M/C2743a.java |
| https://forums.lanik.us/viewforum.php?f=91\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/liste\_fr.txt\ | M/C2743a.java |
| https://www.zoso.ro/rolist\ | M/C2743a.java |
| https://www.zoso.ro/pages/rolist.txt\ | M/C2743a.java |
| https://easylist.to/easylist/easyprivacy.txt\ | M/C2743a.java |
| https://adblock.gardar.net/\ | M/C2743a.java |
| https://adblock.gardar.net/is.abp.txt\ | M/C2743a.java |
| https://github.com/realodix/AdBlockID\ | M/C2743a.java |
| https://raw.githubusercontent.com/realodix/AdBlockID/master/output/adblockid.txt\ | M/C2743a.java |
| https://github.com/kargig/greek-adblockplus-filter\ | M/C2743a.java |
| https://www.void.gr/kargig/void-gr-filters.txt\ | M/C2743a.java |
| https://secure.fanboy.co.nz/fanboy-annoyance\_ubo.txt\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/fanboy-social.txt\ | M/C2743a.java |
| https://github.com/yourduskquibbles/webannoyances/\ | M/C2743a.java |
| https://raw.githubusercontent.com/yourduskquibbles/webannoyances/master/ultralist.txt\ | M/C2743a.java |
| https://github.com/easylist-thailand/\ | M/C2743a.java |
| https://raw.githubusercontent.com/easylist-thailand/easylist-thailand/master/subscription/easylist-thailand.txt\ | M/C2743a.java |
| https://github.com/hufilter/hufilter/wiki\ | M/C2743a.java |
| https://raw.githubusercontent.com/hufilter/hufilter/master/hufilter-adguard.txt\ | M/C2743a.java |
| https://pgl.yoyo.org/adservers/\ | M/C2743a.java |
| https://pgl.yoyo.org/adservers/serverlist.php?hostformat=adblockplus&mimetype=plaintext\ | M/C2743a.java |
| https://xfiles.noads.it/\ | M/C2743a.java |
| https://raw.githubusercontent.com/gioxx/xfiles/master/filtri.txt\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/antiadblockfilters.txt\ | M/C2743a.java |
| https://gitlab.com/malware-filter/urlhaus-filter | M/C2743a.java |
| https://malware-filter.gitlab.io/malware-filter/urlhaus-filter-ag-online.txt\ | M/C2743a.java |
| https://github.com/banbendalao/ADgk\ | M/C2743a.java |
| https://raw.githubusercontent.com/banbendalao/ADgk/master/ADgk.txt\ | M/C2743a.java |
| https://forums.lanik.us/viewforum.php?f=102\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/cntblock.txt\ | M/C2743a.java |
| https://abpvn.com/\ | M/C2743a.java |
| https://raw.githubusercontent.com/abpvn/abpvn/master/filter/abpvn\_adguard.txt\ | M/C2743a.java |
| https://secure.fanboy.co.nz/\ | M/C2743a.java |
| https://secure.fanboy.co.nz/enhancedstats.txt\ | M/C2743a.java |
| https://github.com/MajkiIT/polish-ads-filter | M/C2743a.java |
| https://raw.githubusercontent.com/MajkiIT/polish-ads-filter/master/polish-adblock-filters/adblock.txt\ | M/C2743a.java |
| https://raw.githubusercontent.com/MajkiIT/polish-ads-filter/master/cookies\_filters/adblock\_cookies.txt\ | M/C2743a.java |
| https://adblock.ee/\ | M/C2743a.java |
| https://adblock.ee/list.php\ | M/C2743a.java |
| http://abpchina.org/forum/forum.php?mod=viewthread&tid=29667\ | M/C2743a.java |
| https://raw.githubusercontent.com/cjx82630/cjxlist/master/cjx-annoyance.txt\ | M/C2743a.java |
| https://raw.githubusercontent.com/MajkiIT/polish-ads-filter/master/adblock\_social\_filters/adblock\_social\_list.txt\ | M/C2743a.java |
| https://www.fanboy.co.nz\ | M/C2743a.java |
| https://www.fanboy.co.nz/fanboy-antifacebook.txt\ | M/C2743a.java |
| https://list-kr.github.io/\ | M/C2743a.java |
| https://raw.githubusercontent.com/List-KR/List-KR/master/filter.txt\ | M/C2743a.java |
| https://github.com/xinggsf/Adblock-Plus-Rule/\ | M/C2743a.java |
| https://raw.githubusercontent.com/xinggsf/Adblock-Plus-Rule/master/rule.txt\ | M/C2743a.java |
| https://www.i-dont-care-about-cookies.eu/\ | M/C2743a.java |
| https://www.i-dont-care-about-cookies.eu/abp/\ | M/C2743a.java |
| https://hg.adblockplus.org/easylistspanish\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/easylistspanish.txt\ | M/C2743a.java |
| https://github.com/FiltersHeroes/KAD\ | M/C2743a.java |
| https://raw.githubusercontent.com/FiltersHeroes/KAD/master/KAD.txt\ | M/C2743a.java |
| https://github.com/theel0ja/finnish-easylist-addition\ | M/C2743a.java |
| https://raw.githubusercontent.com/theel0ja/finnish-easylist-addition/master/Finland\_adb.txt\ | M/C2743a.java |
| https://zoso.ro/rolist/\ | M/C2743a.java |
| https://www.zoso.ro/pages/rolist2.txt\ | M/C2743a.java |
| https://github.com/MasterKia/PersianBlocker/\ | M/C2743a.java |
| https://raw.githubusercontent.com/MasterKia/PersianBlocker/main/PersianBlocker.txt\ | M/C2743a.java |
| https://github.com/tcptomato/ROad-Block\ | M/C2743a.java |
| https://raw.githubusercontent.com/tcptomato/ROad-Block/master/road-block-filters-light.txt\ | M/C2743a.java |
| https://polishannoyancefilters.netlify.app\ | M/C2743a.java |
| https://raw.githubusercontent.com/PolishFiltersTeam/PolishAnnoyanceFilters/master/PPB.txt\ | M/C2743a.java |
| https://github.com/olegwukr/polish-privacy-filters\ | M/C2743a.java |
| https://raw.githubusercontent.com/olegwukr/polish-privacy-filters/master/anti-adblock.txt\ | M/C2743a.java |
| https://www.fanboy.co.nz/\ | M/C2743a.java |
| https://fanboy.co.nz/fanboy-antifonts.txt\ | M/C2743a.java |
| https://www.fanboy.co.nz/fanboy-cookiemonster.txt\ | M/C2743a.java |
| https://github.com/hoshsadiq/adblock-nocoin-list/\ | M/C2743a.java |
| https://raw.githubusercontent.com/hoshsadiq/adblock-nocoin-list/master/nocoin.txt\ | M/C2743a.java |
| https://github.com/lassekongo83/Frellwit-s-filter-lists\ | M/C2743a.java |
| https://raw.githubusercontent.com/lassekongo83/Frellwits-filter-lists/master/Frellwits-Swedish-Filter.txt\ | M/C2743a.java |
| https://github.com/yous/YousList/\ | M/C2743a.java |
| https://raw.githubusercontent.com/yous/YousList/master/youslist.txt\ | M/C2743a.java |
| https://github.com/maciejtarmas/AlleBlock\ | M/C2743a.java |
| https://alleblock.pl/alleblock/alleblock.txt\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/easylistpolish.txt\ | M/C2743a.java |
| https://github.com/PolishFiltersTeam/PolishAntiAnnoyingSpecialSupplement\ | M/C2743a.java |
| https://raw.githubusercontent.com/PolishFiltersTeam/PolishAntiAnnoyingSpecialSupplement/master/polish\_rss\_filters.txt\ | M/C2743a.java |
| https://github.com/DandelionSprout/adfilt\ | M/C2743a.java |
| https://raw.githubusercontent.com/DandelionSprout/adfilt/master/NorwegianExperimentalList%20alternate%20versions/NordicFiltersAdGuard.txt\ | M/C2743a.java |
| https://raw.githubusercontent.com/DandelionSprout/adfilt/master/AnnoyancesList\ | M/C2743a.java |
| https://raw.githubusercontent.com/DandelionSprout/adfilt/master/LegitimateURLShortener.txt\ | M/C2743a.java |
| https://raw.githubusercontent.com/DandelionSprout/adfilt/master/SerboCroatianList.txt\ | M/C2743a.java |
| https://github.com/mediumkreation/IndianList\ | M/C2743a.java |
| https://easylist-downloads.adblockplus.org/indianlist.txt\ | M/C2743a.java |
| https://kb.adguard.com/general/search-ads-and-self-promotion\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/10\_optimized.txt\ | M/C2743a.java |
| https://kb.adguard.com/general/adguard-ad-filters\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/11\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/13\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/14\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/15\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/16\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/17\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/18\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/19\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/1\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/20\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/21\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/224\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/22\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/2\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/3\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/4\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/5\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/6\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/7\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/8\_optimized.txt\ | M/C2743a.java |
| https://filters.adtidy.org/android/filters/9\_optimized.txt\ | M/C2743a.java |
| http://logback.qos.ch/css/classic.css | ch/qos/logback/classic/html/UrlCssBuilder.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/classic/net/SocketReceiver.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/CoreConstants.java |
| http://logback.qos.ch/manual/ | ch/qos/logback/core/CoreConstants.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/FileAppender.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/OutputStreamAppender.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/joran/action/AppenderRefAction.java |
| http://xml.org/sax/features/validation | ch/qos/logback/core/joran/event/SaxEventRecorder.java |
| http://xml.org/sax/features/namespaces | ch/qos/logback/core/joran/event/SaxEventRecorder.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/net/SyslogAppenderBase.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/net/AbstractSocketAppender.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/net/SMTPAppenderBase.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/SizeBasedTriggeringPolicy.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/TimeBasedRollingPolicy.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/RollingFileAppender.java |
| http://logback.qos.ch/manual/appenders.html | ch/qos/logback/core/rolling/SizeAndTimeBasedFNATP.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/FixedWindowRollingPolicy.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/TimeBasedFileNamingAndTriggeringPolicyBase.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/rolling/helper/RenameUtil.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/pattern/parser/Parser.java |
| http://logback.qos.ch/codes.html | ch/qos/logback/core/sift/SiftingJoranConfiguratorBase.java |
| https://userscripts.adtidy.org/release/adguard-extra/1.0/adguard-extra.user.js | com/adguard/android/storage/B.java |
| https://userscripts.adtidy.org/release/disable-amp/1.0/disable-amp.user.js | com/adguard/android/storage/B.java |
| http://javax.xml.XMLConstants/feature/secure-processing | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| http://apache.org/xml/features/disallow-doctype-decl | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | com/fasterxml/jackson/databind/ext/DOMDeserializer.java |
| https://play.google.com/store/apps/details?id= | l4/j.java |
| http://www.slf4j.org/codes.html | H8/e.java |
| http://www.slf4j.org/codes.html | H8/d.java |
| http://logback.qos.ch/codes.html | K8/a.java |
| https://m.youtube.com | x5/C8120a.java |
| https://youtube.com/watch?v= | y5/f.java |
| https://www.youtube.com/watch?v= | y5/f.java |
| https://m.youtube.com/watch?v= | y5/f.java |
| https://youtu.be/ | y5/f.java |
| https://youtube.com/shorts/ | y5/f.java |
| https://www.youtube.com/shorts/ | y5/f.java |
| https://m.youtube.com/shorts/ | y5/f.java |
| https://youtube.com/live/ | y5/f.java |
| https://www.youtube.com/live/ | y5/f.java |
| https://m.youtube.com/live/ | y5/f.java |
| https://f-droid.org/repository/browse/?fdid=org.torproject.android | g0/C7061b.java |
| https://www.youtube.com/watch?v= | z2/g.java |
| https://github.com/L-JINBIN/ApkSignatureKillerEx | bin/mt/signature/KillerApplication.java |
| https://dns.adguard.com/dns-query | V/a.java |
| https://dns.adguard-dns.com/dns-query | V/a.java |
| https://dns-family.adguard.com/dns-query | V/a.java |
| https://family.adguard-dns.com/dns-query | V/a.java |
| https://dns-unfiltered.adguard.com/dns-query | V/a.java |
| https://unfiltered.adguard-dns.com/dns-query | V/a.java |
| https://filters.adtidy.org/android/filters/17\_optimized.txt\ | c0/C6414a.java |
| https://kb.adguard.com/general/adguard-ad-filters\ | c0/C6414a.java |

### **4.3 邮箱线索**

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 13022222222 | F/c.java |
| 13122222222 | F/c.java |
| 13222222222 | F/c.java |
| 13322222222 | F/c.java |
| 13422222222 | F/c.java |
| 13522222222 | F/c.java |
| 13622222222 | F/c.java |
| 13722222222 | F/c.java |
| 13822222222 | F/c.java |
| 13922222222 | F/c.java |
| 14022222222 | F/c.java |
| 14122222222 | F/c.java |
| 14222222222 | F/c.java |
| 14322222222 | F/c.java |
| 14422222222 | F/c.java |
| 14522222222 | F/c.java |
| 14622222222 | F/c.java |
| 14722222222 | F/c.java |
| 14822222222 | F/c.java |
| 14922222222 | F/c.java |
| 15022222222 | F/c.java |
| 15122222222 | F/c.java |
| 15222222222 | F/c.java |
| 15322222222 | F/c.java |
| 15422222222 | F/c.java |
| 15522222222 | F/c.java |
| 15622222222 | F/c.java |
| 15722222222 | F/c.java |
| 15822222222 | F/c.java |
| 15922222222 | F/c.java |
| 16022222222 | F/c.java |
| 16122222222 | F/c.java |
| 16222222222 | F/c.java |
| 16322222222 | F/c.java |
| 16422222222 | F/c.java |
| 16522222222 | F/c.java |
| 16622222222 | F/c.java |
| 17222222222 | F/c.java |
| 18222222222 | F/c.java |
| 19222222222 | F/c.java |
| 16722222222 | F/c.java |
| 16822222222 | F/c.java |
| 16922222222 | F/c.java |
| 17022222222 | F/c.java |
| 17122222222 | F/c.java |
| 17322222222 | F/c.java |
| 17422222222 | F/c.java |
| 17522222222 | F/c.java |
| 17622222222 | F/c.java |
| 17722222222 | F/c.java |
| 17822222222 | F/c.java |
| 17922222222 | F/c.java |
| 18022222222 | F/c.java |
| 18122222222 | F/c.java |
| 18322222222 | F/c.java |
| 18422222222 | F/c.java |
| 18522222222 | F/c.java |
| 18622222222 | F/c.java |
| 18722222222 | F/c.java |
| 18822222222 | F/c.java |
| 18922222222 | F/c.java |
| 19022222222 | F/c.java |
| 19122222222 | F/c.java |
| 19322222222 | F/c.java |
| 19422222222 | F/c.java |
| 19522222222 | F/c.java |
| 19622222222 | F/c.java |
| 19722222222 | F/c.java |
| 19822222222 | F/c.java |
| 19922222222 | F/c.java |
| 15222222222 | T/a.java |
| 16222222222 | T/a.java |
| 19222222222 | T/a.java |
| 18222222222 | T/a.java |
| 13222222222 | T/a.java |
| 14222222222 | T/a.java |
| 17222222222 | T/a.java |
| 17322222222 | T/a.java |
| 17422222222 | T/a.java |
| 17522222222 | T/a.java |
| 17622222222 | T/a.java |
| 17722222222 | T/a.java |
| 17822222222 | T/a.java |
| 17922222222 | T/a.java |
| 18022222222 | T/a.java |
| 18122222222 | T/a.java |
| 18322222222 | T/a.java |
| 18422222222 | T/a.java |
| 18522222222 | T/a.java |
| 18622222222 | T/a.java |
| 18722222222 | T/a.java |
| 18822222222 | T/a.java |
| 18922222222 | T/a.java |
| 19022222222 | T/a.java |
| 19122222222 | T/a.java |
| 19322222222 | T/a.java |
| 19422222222 | T/a.java |
| 19522222222 | T/a.java |
| 19622222222 | T/a.java |
| 19722222222 | T/a.java |
| 19822222222 | T/a.java |
| 19922222222 | T/a.java |

## **5. 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=Texas, ST=TX, L=Beasley, O=APKMODY, OU=APKMODY, CN=Anh Pham 签名算法: rsassa\_pkcs1v15 有效期自: 2021-12-24 04:00:59+00:00 有效期至: 2046-12-18 04:00:59+00:00 发行人: C=Texas, ST=TX, L=Beasley, O=APKMODY, OU=APKMODY, CN=Anh Pham 序列号: 0x146ca459 哈希算法: sha256 md5值: 646d852e31272e772fe24985be2033c9 sha1值: 1cc63a91d447918eea7e38042c54e6068dcaeae3 sha256值: 358020b0ed9d910c3eb4e03e261eb340604833f8bdc75e236d965e80e63a56de sha512值: 4b1e16e596fcf39b5f5b97c3725c334db5e9df4129498dcc7539f806f0ae02aaa796d6397177c6cda3168ccd8c23168df9637664f989497f404763fb91ed996b 公钥算法: rsa 密钥长度: 2048 指纹: ff628834313df85c8f4bcfb73cf66b30f8adcd427cf1de3dfd3c167d5f333ac1**

## **6. 硬编码敏感信息**

## **7. 加壳分析**

| 加壳类型 | 所属文件 |
| --- | --- |
| 登陆摸瓜网站后查看 |  |

## **8. 第三方插件**

| 名称 | 分类 | URL链接 |
| --- | --- | --- |
| 登陆摸瓜网站后查看 |  |  |

## **9. 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\_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.INTERACT\_ACROSS\_USERS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.BLUETOOTH\_CONNECT | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.PACKAGE\_USAGE\_STATS | 合法 | 更新组件使用统计 | 允许修改收集的组件使用统计。不供普通应用程序使用 |
| 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.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.RECEIVE\_BOOT\_COMPLETED | 正常 | 开机时自动启动 | 允许应用程序在系统完成启动后立即启动。这可能会使启动手机需要更长的时间,并允许应用程序通过始终运行来减慢整个手机的速度 |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_SYSTEM\_EXEMPTED | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_DATA\_SYNC | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS | 正常 |  | 应用程序必须持有的权限才能使用 Settings.ACTION\_REQUEST\_IGNORE\_BATTERY\_OPTIMIZATIONS。 |
| 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 |
| android.permission.SCHEDULE\_EXACT\_ALARM | 正常 |  | 允许应用程序使用精确的警报调度 API 来执行对时间敏感的后台工作 |
| android.permission.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| 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.adguard.android.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| 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\_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 |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| com.adguard.android.ui.activity.AdGuardSchemeSortingActivity | **Schemes**: adguard://, |
| com.adguard.android.ui.activity.SdnsSchemeSortingActivity | **Schemes**: sdns://, |
| com.adguard.android.ui.activity.FiltersSubscriptionSchemeSortingActivity | **Schemes**: adg://, abp://, https://, http://,  **Hosts:** subscribe.adblockplus.org, |
| com.adguard.android.ui.activity.PrivateBrowserRoutingActivity | **Schemes**: http://, https://,  **Mime Types:** text/plain, |
| com.adguard.android.ui.activity.YoutubeRoutingActivity | **Schemes**: http://, https://,  **Hosts:** youtu.be, m.youtube.com, youtube.com, www.youtube.com,  **Mime Types:** text/plain, |

**报告由**  [**摸瓜APK反编译平台**](https://mogua.co)  **自动生成，并非包含所有检测结果，有疑问请联系管理员。**