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

**LVCHA VPN（ 2.6.1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 | LVCHA VPN |
| 版本 | 2.6.1 |
| 包名 | com.abilvcha.main |
| 域名线索 | 170条 |
| URL线索 | 16条 |
| APP图标 |  |
| 分析日期 | 2025年8月4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 | 绿茶VPN.apk |
| 文件大小 | 5.02MB |
| MD5值 | 5f96f4fbf085b928b038d563c418c002 |
| SHA1值 | d7c3790e0d2b9ce79d8bb36ddc16507979528860 |
| SHA256值 | 86157dee1b561ec00ccead32e51bb179b74a4ac66cc5b38e23204c58d0a7d2d5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | LVCHA VPN |
| 包名 | com.abilvcha.main |
| 主活动Activity | com.lvcha.main.activity.WelcomeActivity |
| 安卓版本名称 | 2.6.1 |
| 安卓版本 | 29 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| www.dailymotion.com | IP: 199.59.149.136  所属国家: United States of America  地区: California  城市: San Francisco |
| goo.gl | IP: 142.250.217.78  所属国家: United States of America  地区: California  城市: Mountain View |
| www.mozilla.org | IP: 151.101.91.19  所属国家: United States of America  地区: California  城市: San Francisco |
| www.tumblr.com | IP: 128.242.240.29  所属国家: United States of America  地区: Washington  城市: Redmond |
| tubitv.com | IP: 18.164.174.19  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.pubgmobile.com | IP: 92.122.244.51  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| www.facebook.com | IP: 108.160.162.104  所属国家: United States of America  地区: California  城市: San Francisco |
| www.netflix.com | IP: 52.38.7.83  所属国家: United States of America  地区: Oregon  城市: Portland |
| www.zongheng.com | IP: 59.110.246.214  所属国家: China  地区: Beijing  城市: Beijing |
| www.thetrainline.com | IP: 18.154.206.94  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.nordstrom.com | IP: 151.101.90.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.microsoft.com | IP: 221.194.156.64  所属国家: China  地区: Hebei  城市: Langfang |
| character.ai | IP: 199.96.58.177  所属国家: United States of America  地区: California  城市: San Francisco |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| planetix.com | IP: 104.21.45.7  所属国家: United States of America  地区: California  城市: San Francisco |
| www.dc.com | IP: 151.101.89.55  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 |
| sp.nicovideo.jp | IP: 104.244.46.52  所属国家: United States of America  地区: California  城市: San Francisco |
| www.shixinfo.com | IP: 39.108.2.129  所属国家: China  地区: Guangdong  城市: Shenzhen |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| wildrift.leagueoflegends.com | IP: 3.33.186.135  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.notion.so | IP: 208.103.161.2  所属国家: United States of America  地区: South Carolina  城市: Mount Pleasant |
| www.dmm.com | IP: 18.65.27.57  所属国家: United States of America  地区: California  城市: Los Angeles |
| twitter.com | IP: 199.59.148.229  所属国家: United States of America  地区: California  城市: San Francisco |
| www.grailed.com | IP: 104.16.234.118  所属国家: United States of America  地区: California  城市: San Francisco |
| meet.google.com | IP: 142.250.73.110  所属国家: United States of America  地区: California  城市: Mountain View |
| www.grab.com | IP: 18.65.25.9  所属国家: United States of America  地区: California  城市: Los Angeles |
| pimeyes.com | IP: 162.125.32.2  所属国家: United States of America  地区: California  城市: San Francisco |
| www.outwrite.com | IP: 76.76.21.142  所属国家: United States of America  地区: California  城市: Walnut |
| copy.ai | IP: 34.217.231.110  所属国家: United States of America  地区: Oregon  城市: Portland |
| fate-go.us | IP: 3.167.192.54  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.toptoon.net | IP: 50.117.117.42  所属国家: United States of America  地区: California  城市: Santa Clara |
| www.flickr.com | IP: 128.121.146.101  所属国家: United States of America  地区: California  城市: Sacramento |
| www.walmart.com | IP: 23.55.208.195  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| vk.com | IP: 87.240.129.133  所属国家: Russian Federation  地区: Sankt-Peterburg  城市: Saint Petersburg |
| smodin.io | IP: 34.117.39.253  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.reddit.com | IP: 108.160.172.232  所属国家: United States of America  地区: California  城市: San Francisco |
| www.google.com | IP: 199.59.148.20  所属国家: United States of America  地区: California  城市: San Francisco |
| www.threads.net | IP: 31.13.94.10  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.booking.com | IP: 18.164.174.74  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.theguardian.com | IP: 151.101.89.111  所属国家: United States of America  地区: California  城市: San Francisco |
| www.feixiaohao.com | IP: 104.244.43.234  所属国家: United States of America  地区: California  城市: San Francisco |
| zoom.earth | IP: 104.26.4.90  所属国家: United States of America  地区: California  城市: San Francisco |
| 17.live | IP: 104.244.43.208  所属国家: United States of America  地区: California  城市: San Francisco |
| www.sephora.com | IP: 23.219.68.100  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.viu.com | IP: 3.168.136.245  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.kakaocorp.com | IP: 211.249.221.227  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.gate.io | IP: 127.0.0.1  所属国家: -  地区: -  城市: - |
| time.com | IP: 75.126.33.156  所属国家: United States of America  地区: California  城市: San Jose |
| www.huffpost.com | IP: 157.240.20.18  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| zoom.us | IP: 170.114.52.2  所属国家: United States of America  地区: California  城市: San Jose |
| app.ejsen.cn | IP: 154.194.161.185  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| shopee.com | IP: 143.92.82.21  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.pinterest.com | IP: 69.63.180.173  所属国家: United States of America  地区: California  城市: Menlo Park |
| genshin.hoyoverse.com | IP: 3.169.252.86  所属国家: United States of America  地区: Washington  城市: Seattle |
| tinder.com | IP: 52.84.150.39  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.suruga-ya.com | IP: 31.13.64.7  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.foxnews.com | IP: 23.218.94.219  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.worldcoinindex.com | IP: 104.26.14.233  所属国家: United States of America  地区: California  城市: San Francisco |
| play.google.com | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| www.camfrog.com | IP: 118.193.202.219  所属国家: China  地区: Beijing  城市: Beijing |
| www.afreecatv.com | IP: 118.218.124.193  所属国家: Korea (Republic of)  地区: Seoul-teukbyeolsi  城市: Seoul |
| www.marvel.com | IP: 3.167.192.26  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.wsj.com | IP: 199.59.149.136  所属国家: United States of America  地区: California  城市: San Francisco |
| www.binance.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| www.coupang.com | IP: 23.209.177.222  所属国家: Australia  地区: New South Wales  城市: Sydney |
| slack.com | IP: 52.192.46.121  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.telltale.com | IP: 173.236.159.172  所属国家: United States of America  地区: California  城市: Brea |
| arabic.nsfx.com | IP: 18.197.205.127  所属国家: Germany  地区: Hessen  城市: Frankfurt am Main |
| app-measurement.com | IP: 114.250.63.33  所属国家: China  地区: Beijing  城市: Beijing |
| lubansms.com | IP: 172.67.74.40  所属国家: United States of America  地区: California  城市: San Francisco |
| www.sudowrite.com | IP: 216.24.57.1  所属国家: United States of America  地区: California  城市: San Francisco |
| ethermine.org | IP: 31.13.106.4  所属国家: Ireland  地区: Dublin  城市: Dublin |
| mail.google.com | IP: 142.250.217.69  所属国家: United States of America  地区: California  城市: Mountain View |
| www.mercari.com | IP: 103.252.115.49  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.imdb.com | IP: 18.164.175.229  所属国家: United States of America  地区: California  城市: Los Angeles |
| www3.nhk.or.jp | IP: 23.209.176.176  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.hulu.com | IP: 23.193.119.203  所属国家: United States of America  地区: California  城市: San Jose |
| zapier.com | IP: 3.168.147.19  所属国家: United States of America  地区: Washington  城市: Seattle |
| web.telegram.org | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| www.lazada.com | IP: 155.102.4.6  所属国家: United States of America  地区: California  城市: San Mateo |
| www.maxmovie.com | IP: 3.34.19.53  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Icheon |
| www.potato.im | IP: 157.240.9.36  所属国家: Bulgaria  地区: Sofia (stolitsa)  城市: Sofia |
| coinw.zendesk.com | IP: 104.18.249.37  所属国家: United States of America  地区: California  城市: San Francisco |
| www.ebay.com | IP: 23.209.177.65  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.agedm.org | IP: 23.225.30.102  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.chinatimes.com | IP: 172.66.140.98  所属国家: United States of America  地区: California  城市: San Francisco |
| vimeo.com | IP: 31.13.94.37  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.cz01.vip | IP: 45.154.214.60  所属国家: United States of America  地区: Washington  城市: Seattle |
| jumpshop-online.com | IP: 23.227.38.65  所属国家: Canada  地区: Ontario  城市: Ottawa |
| scholar.google.com | IP: 142.250.69.164  所属国家: United States of America  地区: California  城市: Mountain View |
| www.canva.com | IP: 104.16.102.112  所属国家: United States of America  地区: California  城市: San Francisco |
| www.grammarly.com | IP: 18.154.144.104  所属国家: United States of America  地区: California  城市: Los Angeles |
| metamask.io | IP: 108.160.167.158  所属国家: United States of America  地区: California  城市: San Francisco |
| www.ea.com | IP: 23.209.176.157  所属国家: Australia  地区: New South Wales  城市: Sydney |
| www.rakuten.co.jp | IP: 174.37.54.20  所属国家: United States of America  地区: California  城市: San Jose |
| www.yahoo.com | IP: 69.147.80.12  所属国家: United States of America  地区: New York  城市: New York City |
| www.xe.com | IP: 3.163.125.72  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.taptap.io | IP: 104.18.1.19  所属国家: United States of America  地区: California  城市: San Francisco |
| discord.com | IP: 128.121.243.77  所属国家: United States of America  地区: Washington  城市: Redmond |
| mir4global.com | IP: 13.72.197.150  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| www.nba2k.com | IP: 192.81.242.63  所属国家: United States of America  地区: New York  城市: New York City |
| www.midjourney.com | IP: 172.64.154.39  所属国家: United States of America  地区: California  城市: San Francisco |
| tw.yahoo.com | IP: 31.13.112.4  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.tradingview.com | IP: 173.255.209.47  所属国家: United States of America  地区: California  城市: Fremont |
| www.wikipedia.org | IP: 31.13.94.41  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.drivethrucomics.com | IP: 172.67.196.233  所属国家: United States of America  地区: California  城市: San Francisco |
| www.youtube.com | IP: 31.13.88.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.shiekhshoes.com | IP: 52.88.254.241  所属国家: United States of America  地区: Oregon  城市: Boardman |
| nikke.hotcool.tw | IP: 104.21.43.36  所属国家: United States of America  地区: California  城市: San Francisco |
| www.chatgpt.com | IP: 69.171.229.73  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.pixiv.net | IP: 157.240.1.50  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.gocomics.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| edition.cnn.com | IP: 151.101.3.5  所属国家: United States of America  地区: California  城市: San Francisco |
| www.htx.com | IP: 199.59.148.7  所属国家: United States of America  地区: California  城市: San Francisco |
| runwayml.com | IP: 76.76.21.21  所属国家: United States of America  地区: California  城市: Walnut |
| chat.openai.com | IP: 31.13.94.23  所属国家: Argentina  地区: Ciudad Autonoma de Buenos Aires  城市: Buenos Aires |
| www.naver.com | IP: 223.130.192.247  所属国家: Korea (Republic of)  地区: Gyeonggi-do  城市: Seongnam |
| www.marvelsuperwar.com | 没有服务器地理信息. |
| www.disney.com | IP: 23.193.119.140  所属国家: United States of America  地区: California  城市: San Jose |
| www.tvbanywhere.com | IP: 3.167.192.57  所属国家: United States of America  地区: Washington  城市: Seattle |
| sms-activate.org | IP: 104.26.12.90  所属国家: United States of America  地区: California  城市: San Francisco |
| zenly.com | IP: 34.120.54.238  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.mail.com | IP: 74.208.232.20  所属国家: United States of America  地区: Pennsylvania  城市: Philadelphia |
| opensea.io | IP: 199.59.148.6  所属国家: United States of America  地区: California  城市: San Francisco |
| www.googleadservices.com | IP: 114.250.65.38  所属国家: China  地区: Beijing  城市: Beijing |
| www.skype.com | IP: 52.113.194.133  所属国家: United States of America  地区: Washington  城市: Redmond |
| myspace.com | IP: 34.111.176.156  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.nexon.com | IP: 52.84.150.40  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.quora.com | IP: 199.59.150.13  所属国家: United States of America  地区: California  城市: San Francisco |
| mixi.jp | IP: 128.242.240.212  所属国家: United States of America  地区: Washington  城市: Redmond |
| cn.nytimes.com | IP: 104.244.43.208  所属国家: United States of America  地区: California  城市: San Francisco |
| line.me | IP: 128.121.243.235  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.instagram.com | IP: 96.44.137.28  所属国家: United States of America  地区: California  城市: Los Angeles |
| www.walgreens.com | IP: 23.210.26.173  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| m.iyf.tv | IP: 104.18.33.187  所属国家: United States of America  地区: California  城市: San Francisco |
| token.im | IP: 104.20.45.246  所属国家: United States of America  地区: California  城市: San Francisco |
| www.twitch.tv | IP: 31.13.76.99  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.deepl.com | IP: 172.64.148.47  所属国家: United States of America  地区: California  城市: San Francisco |
| pagead2.googlesyndication.com | IP: 114.250.66.38  所属国家: China  地区: Beijing  城市: Beijing |
| google.com | IP: 46.82.174.69  所属国家: Germany  地区: Niedersachsen  城市: Braunschweig |
| www.tokenpocket.pro | IP: 74.86.228.110  所属国家: United States of America  地区: California  城市: San Jose |
| www.tiktok.com | IP: 202.160.128.40  所属国家: Singapore  地区: Singapore  城市: Singapore |
| www.messenger.com | IP: 173.231.12.107  所属国家: United States of America  地区: Utah  城市: Ogden |
| bard.google.com | IP: 142.251.33.78  所属国家: Canada  地区: Ontario  城市: Toronto |
| www.coinbase.com | IP: 116.89.243.8  所属国家: China  地区: Henan  城市: Zhengzhou |
| www.bbc.com | IP: 157.240.9.36  所属国家: Bulgaria  地区: Sofia (stolitsa)  城市: Sofia |
| www.voachinese.com | IP: 69.171.229.73  所属国家: United States of America  地区: California  城市: Menlo Park |
| stablediffusionweb.com | IP: 69.171.242.11  所属国家: United States of America  地区: New York  城市: New York City |
| www.toranoana.jp | IP: 52.192.218.43  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| www.okx.com | IP: 0.0.0.0  所属国家: -  地区: -  城市: - |
| www.dw.com | IP: 157.240.18.18  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.cryptocompare.com | IP: 104.18.31.136  所属国家: United States of America  地区: California  城市: San Francisco |
| www.bing.com | IP: 202.89.233.100  所属国家: China  地区: Beijing  城市: Beijing |
| www.whatsapp.com | IP: 118.193.240.41  所属国家: China  地区: Beijing  城市: Beijing |
| www.amazon.com | IP: 18.154.130.13  所属国家: United States of America  地区: California  城市: Los Angeles |
| ani.gamer.com.tw | IP: 104.244.46.85  所属国家: United States of America  地区: California  城市: San Francisco |
| www.linkedin.com | IP: 52.131.37.152  所属国家: China  地区: Beijing  城市: Beijing |
| drive.google.com | IP: 192.133.77.197  所属国家: United States of America  地区: California  城市: San Francisco |
| www.dlsite.com | IP: 38.121.72.166  所属国家: United States of America  地区: Georgia  城市: Atlanta |
| javax.xml.xmlconstants | 没有服务器地理信息. |
| stackoverflow.com | IP: 104.18.32.7  所属国家: United States of America  地区: California  城市: San Francisco |
| www.olevod.com | IP: 108.160.162.102  所属国家: United States of America  地区: California  城市: San Francisco |
| firebase.google.com | IP: 142.250.73.78  所属国家: United States of America  地区: California  城市: Mountain View |
| firebase-settings.crashlytics.com | IP: 114.250.64.34  所属国家: China  地区: Beijing  城市: Beijing |
| crowd1.com | IP: 104.18.1.188  所属国家: United States of America  地区: California  城市: San Francisco |
| store.steampowered.com | IP: 23.215.161.136  所属国家: Australia  地区: South Australia  城市: Adelaide |
| www.snapchat.com | IP: 34.149.46.130  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| www.apkpure.net | IP: 104.20.43.26  所属国家: United States of America  地区: California  城市: San Francisco |
| android.googlesource.com | IP: 74.125.20.82  所属国家: United States of America  地区: California  城市: Mountain View |

### **4.2 URL线索**

| URL信息 | Url所在文件 |
| --- | --- |
| https://github.com/FasterXML/jackson-databind/issues/2715 | com/fasterxml/jackson/databind/PropertyNamingStrategy.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 |
| http://javax.xml.XMLConstants/feature/secure-processing | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| http://javax.xml.XMLConstants/property/accessExternalDTD | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | com/fasterxml/jackson/databind/ext/DOMSerializer.java |
| https://www.tiktok.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.youtube.com\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://twitter.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.instagram.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.facebook.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://web.telegram.org\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.voachinese.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.netflix.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.amazon.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.binance.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.apkpure.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://chat.openai.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.pixiv.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.bbc.com/zhongwen/simp\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.wikipedia.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://line.me/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.twitch.tv/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://store.steampowered.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://play.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://github.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.disney.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.hulu.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.chatgpt.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://character.ai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://bard.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://runwayml.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grammarly.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.midjourney.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.sudowrite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.outwrite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://copy.ai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.canva.com/design/play\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.notion.so/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zapier.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://smodin.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://stablediffusionweb.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://github.com/features/copilot\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://vimeo.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tvbanywhere.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.olevod.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.viu.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.imdb.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://m.iyf.tv/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tubitv.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.cz01.vip/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://17.live/en\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.afreecatv.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.maxmovie.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dailymotion.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dlsite.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://jumpshop-online.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://ani.gamer.com.tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://sp.nicovideo.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.suruga-ya.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.toptoon.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dmm.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.agedm.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dc.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.marvel.com/unlimited\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.amazon.com/kindle-dbs/comics-store/home\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.drivethrucomics.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.toranoana.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.gocomics.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.zongheng.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.chinatimes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tw.yahoo.com/?p=dnr\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://cn.nytimes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.quora.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.dw.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.foxnews.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www3.nhk.or.jp/nhkworld/zh/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.reddit.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://edition.cnn.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://time.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.theguardian.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.huffpost.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.wsj.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.threads.net/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://web.telegram.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.whatsapp.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://tinder.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.potato.im/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mixi.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.kakaocorp.com/page/?lang=ENG\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.messenger.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://vk.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.camfrog.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.snapchat.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.pinterest.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tumblr.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zenly.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.flickr.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://myspace.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://nikke.hotcool.tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://discord.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.taptap.io/app/154140\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://genshin.hoyoverse.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://wildrift.leagueoflegends.com/zh-tw/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.ea.com/en-gb/games/apex-legends\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mir4global.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.pubgmobile.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://fate-go.us/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nexon.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.marvelsuperwar.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.telltale.com/batman-a-telltale-story/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nba2k.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tradingview.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://app.ejsen.cn/index1.html\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.shixinfo.com/download/ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://coinw.zendesk.com/hc/zh-cn\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.okx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.feixiaohao.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://opensea.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.tokenpocket.pro/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://planetix.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.gate.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.htx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://metamask.io/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://token.im/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://ethermine.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.cryptocompare.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.worldcoinindex.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.coinbase.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://arabic.nsfx.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://shopee.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.coupang.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mercari.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.lazada.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.rakuten.co.jp/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.ebay.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.sephora.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.nordstrom.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grailed.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.walgreens.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| http://www.shiekhshoes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.walmart.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.deepl.com/translator\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.linkedin.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://mail.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://scholar.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://stackoverflow.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zoom.us/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://meet.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://crowd1.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://drive.google.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://slack.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.microsoft.com/en-sg/microsoft-teams/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.skype.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/maps/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.xe.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.booking.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.thetrainline.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.grab.com/cn/xia-zai/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://pimeyes.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.yahoo.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.google.com/chrome/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.bing.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://zoom.earth/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mozilla.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.naver.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://www.mail.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://lubansms.com/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://sms-activate.org/\ | com/lvcha/main/activity/LvchaCircleAPPActivity.java |
| https://pagead2.googlesyndication.com/pagead/gen\_204?id=gmob-apps | defpackage/lz1.java |
| https://app-measurement.com/a | defpackage/st2.java |
| https://firebase.google.com/docs/analytics | defpackage/j72.java |
| https://google.com/search? | defpackage/lm2.java |
| https://app-measurement.com/a | defpackage/z22.java |
| https://firebase.google.com/docs/crashlytics/get-started?platform=android | defpackage/kp.java |
| https://www.google.com | defpackage/lt2.java |
| https://www.googleadservices.com/pagead/conversion/app/deeplink?id\_type=adid&sdk\_version=%s&rdid=%s&bundleid=%s&retry=%s | defpackage/lt2.java |
| https://goo.gl/NAOOOI. | defpackage/lt2.java |
| https://goo.gl/NAOOOI | defpackage/lt2.java |
| https://firebase.google.com/support/privacy/init-options. | defpackage/f40.java |
| https://firebase-settings.crashlytics.com/spi/v2/platforms/android/gmp/%s/settings | defpackage/hg1.java |
| https://firebase.google.com/support/guides/disable-analytics | defpackage/tc2.java |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/property/accessExternalStylesheet | 摸瓜V3引擎 |
| http://schemas.android.com/aapt | 摸瓜V3引擎 |
| https://github.com/fastfloat/fast\_float/blob/35d523195bf7d57aba0e735ad6eba1e6f71ba8d6/LICENSE-MIT | 摸瓜V3引擎 |
| http://www.apache.org/licenses/ | 摸瓜V3引擎 |
| https://github.com/wrandelshofer/FastDoubleParser/blob/39e123b15b71f29a38a087d16a0bc620fc879aa6/bigi | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| http://apache.org/xml/features/nonvalidating/load-external-dtd | 摸瓜V3引擎 |
| https://github.com/tbuktu/bigint/blob/617c8cd8a7c5e4fb4d919c6a4d11e2586107f029/LICENSE | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://github.com/fastfloat/fast\_float | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/property/accessExternalDTD | 摸瓜V3引擎 |
| http://apache.org/xml/features/disallow-doctype-decl | 摸瓜V3引擎 |
| http://javax.xml.XMLConstants/feature/secure-processing | 摸瓜V3引擎 |
| https://github.com/FasterXML/jackson-databind/issues/2715 | 摸瓜V3引擎 |
| https://github.com/tbuktu/bigint/tree/floatfft | 摸瓜V3引擎 |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0  u0013android@android.com | defpackage/ri2.java |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15552000000 | defpackage/yj2.java |

## **5. 签名证书**

**APK已签名 v1 签名: True v2 签名: True v3 签名: False 找到 1 个唯一证书 主题: O=key 签名算法: rsassa\_pkcs1v15 有效期自: 2024-04-19 12:16:40+00:00 有效期至: 2049-04-13 12:16:40+00:00 发行人: O=key 序列号: 0x1 哈希算法: sha256 md5值: a0f4f23a429228ec5ec8f9137cdd79e0 sha1值: 216fedd41a9a538e196be66c1eb6b9a815db0238 sha256值: 100c64083b832a7b374c50037bb28ec6ba4dc679795175eb09861f93dc708c13 sha512值: bbfe1291a201a8d8751dea11c25f4f49da230c26508a156d4ebe80d2c7775856e6f16c4448d5144fc69c868db6e99b7a7907d31d1763b972154f7a95f04695bd 公钥算法: rsa 密钥长度: 2048 指纹: 2a4f7c041d0cf3c1a98e6cf8a4e6bf6d574ca8410110bdf1782d132ef5ad0527**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "com.google.firebase.crashlytics.mapping\_file\_id" : "88256e6c864b4208921bd5d8bc4a1480" |
| "google\_api\_key" : "AIzaSyBFM4MupZpn9SaT8E1N7hPtf83q09Xu8lE" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyBFM4MupZpn9SaT8E1N7hPtf83q09Xu8lE" |
| "unknown\_user" : "Unknown User" |
| "unknown\_user" : "无名用户" |
| "unknown\_user" : "無名用戶" |

## **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.FOREGROUND\_SERVICE\_SYSTEM\_EXEMPTED | 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.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| 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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.ACCESS\_NOTIFICATION\_POLICY | 正常 |  | 希望访问通知策略的应用程序的标记权限。 |
| 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.abilvcha.main.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

**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。**