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

**Telegram X（ 0.26.8.1723-universal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 | Telegram X |
| 版本 | 0.26.8.1723-universal |
| 包名 | org.thunderdog.challegram |
| 域名线索 | 56条 |
| URL线索 | 39条 |
| APP图标 |  |
| 分析日期 | 2025年7月17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 | 19c67d14-ecb1-4231-b009-f28d2120e26a\_telegram-x-0-26-8-1723-universal.apk |
| 文件大小 | 47.44MB |
| MD5值 | 171a1b36b15524762be9bc10ed817025 |
| SHA1值 | e4b251ddaa0bb4136baea0dcd14fb62fd75773a5 |
| SHA256值 | 3332e04cabd18400dee7d568b1dd1c8638bf67295c59488e098d2eeae9b242f5 |

## **3. APP基本信息**

| 类别 | 内容 |
| --- | --- |
| App名称 | Telegram X |
| 包名 | org.thunderdog.challegram |
| 主活动Activity | org.thunderdog.challegram.MainActivity |
| 安卓版本名称 | 0.26.8.1723-universal |
| 安卓版本 | 1723000 |

## **4. 线索情况**

### **4.1 域名线索**

| 域名 | 服务器信息 |
| --- | --- |
| coub.com | IP: 95.213.253.92  所属国家: Russian Federation  地区: Sankt-Peterburg  城市: Saint Petersburg |
| tgb.smart-glocal.com | IP: 75.2.95.23  所属国家: United States of America  地区: Washington  城市: Seattle |
| www.instagram.com | IP: 69.63.184.142  所属国家: United States of America  地区: California  城市: Menlo Park |
| www.apache.org | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| support.google.com | IP: 142.250.73.142  所属国家: United States of America  地区: California  城市: Mountain View |
| foursquare.com | IP: 151.101.2.132  所属国家: United States of America  地区: California  城市: San Francisco |
| www.webrtc.org | IP: 142.250.217.78  所属国家: United States of America  地区: California  城市: Mountain View |
| firebaseinstallations.googleapis.com | IP: 142.250.73.106  所属国家: United States of America  地区: California  城市: Mountain View |
| aomedia.org | IP: 104.244.46.5  所属国家: United States of America  地区: California  城市: San Francisco |
| aomediacodec.github.io | IP: 185.199.109.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| reserve-5a846.firebaseio.com | IP: 35.201.97.85  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| appgallery.huawei.com | IP: 121.36.119.11  所属国家: China  地区: Beijing  城市: Beijing |
| www.w3.org | IP: 104.18.23.19  所属国家: United States of America  地区: California  城市: San Francisco |
| www.ietf.org | IP: 104.16.45.99  所属国家: United States of America  地区: California  城市: San Francisco |
| googlehosted.l.googleusercontent.com | IP: 142.250.73.129  所属国家: United States of America  地区: California  城市: Mountain View |
| crbug.com | IP: 216.239.32.29  所属国家: United States of America  地区: California  城市: Mountain View |
| apps.samsung.com | IP: 104.17.142.17  所属国家: United States of America  地区: California  城市: San Francisco |
| software-download.microsoft.com | IP: 13.107.246.74  所属国家: United States of America  地区: Washington  城市: Redmond |
| webrtc.googlesource.com | IP: 192.178.163.82  所属国家: United States of America  地区: California  城市: Mountain View |
| firebase.google.com | IP: 142.250.73.78  所属国家: United States of America  地区: California  城市: Mountain View |
| telegra.ph | IP: 199.59.148.222  所属国家: United States of America  地区: California  城市: San Francisco |
| ns.adobe.com | 没有服务器地理信息. |
| xmlpull.org | IP: 185.199.110.153  所属国家: United States of America  地区: Pennsylvania  城市: California |
| issuetracker.google.com | IP: 142.251.33.78  所属国家: Canada  地区: Ontario  城市: Toronto |
| ss3.4sqi.net | IP: 151.101.90.132  所属国家: United States of America  地区: California  城市: San Francisco |
| play.google.com | IP: 93.46.8.90  所属国家: Italy  地区: Lombardia  城市: Milan |
| schemas.android.com | 没有服务器地理信息. |
| schemas.microsoft.com | IP: 13.107.246.73  所属国家: United States of America  地区: Washington  城市: Redmond |
| www.youtube.com | IP: 31.13.73.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| tgb-playground.smart-glocal.com | IP: 99.83.179.90  所属国家: United States of America  地区: Washington  城市: Seattle |
| ads.telegram.org | IP: 103.252.115.53  所属国家: Singapore  地区: Singapore  城市: Singapore |
| telegram.org | IP: 192.133.77.133  所属国家: United States of America  地区: California  城市: San Francisco |
| www.example.com | IP: 23.220.68.155  所属国家: Japan  地区: Tokyo  城市: Tokyo |
| music.youtube.com | IP: 31.13.88.26  所属国家: Ireland  地区: Dublin  城市: Dublin |
| www.google.com | IP: 31.13.73.169  所属国家: Ireland  地区: Dublin  城市: Dublin |
| dns.google | IP: 8.8.4.4  所属国家: United States of America  地区: California  城市: Mountain View |
| scenic-parity-125411.firebaseio.com | IP: 34.120.160.131  所属国家: United States of America  地区: Missouri  城市: Kansas City |
| lh3-dz.googleusercontent.com | IP: 142.250.217.97  所属国家: United States of America  地区: California  城市: Mountain View |
| t.me | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| my.telegram.org | IP: 31.13.84.2  所属国家: Austria  地区: Wien  城市: Vienna |
| telesco.pe | IP: 149.154.167.99  所属国家: United Kingdom of Great Britain and Northern Ireland  地区: England  城市: Warrington |
| open.spotify.com | IP: 199.59.148.147  所属国家: United States of America  地区: California  城市: San Francisco |
| music.yandex.ru | IP: 213.180.204.186  所属国家: Russian Federation  地区: Moskva  城市: Moscow |
| default.url | 没有服务器地理信息. |
| plus.google.com | IP: 69.63.180.173  所属国家: United States of America  地区: California  城市: Menlo Park |
| firebaseappcheck.googleapis.com | IP: 142.250.217.74  所属国家: United States of America  地区: California  城市: Mountain View |
| github.com | IP: 20.205.243.166  所属国家: Singapore  地区: Singapore  城市: Singapore |
| translations.telegram.org | IP: 202.160.129.37  所属国家: Singapore  地区: Singapore  城市: Singapore |
| developer.android.com | IP: 142.250.73.110  所属国家: United States of America  地区: California  城市: Mountain View |
| developer.apple.com | IP: 17.253.85.201  所属国家: Hong Kong  地区: Hong Kong  城市: Hong Kong |
| web.telegram.org | IP: 69.63.190.26  所属国家: United States of America  地区: New York  城市: New York City |
| android.googlesource.com | IP: 142.250.99.82  所属国家: United States of America  地区: California  城市: Mountain View |
| firebaseremoteconfig.googleapis.com | IP: 142.251.33.74  所属国家: Canada  地区: Ontario  城市: Toronto |
| g.co | IP: 142.250.73.142  所属国家: United States of America  地区: California  城市: Mountain View |
| twitter.com | IP: 172.66.0.227  所属国家: United States of America  地区: California  城市: San Francisco |
| maps.googleapis.com | IP: 142.250.73.106  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 |
| --- | --- |
| http://ns.adobe.com/xap/1.0/\u0000 | G0/c.java |
| https://github.com/TGX-Android/Telegram-X | I7/C4.java |
| https://www.google.com/maps/search/?api=1&query= | L7/AbstractC1102x.java |
| http://www.example.com | L7/AbstractC1102x.java |
| https://www.google.com/maps/dir/?api=1&destination= | L7/AbstractC1102x.java |
| https://www.example.com/ | L7/AbstractC1102x.java |
| https://play.google.com/store/apps/details?id= | L7/AbstractC1102x.java |
| https://github.com/TGX-Android/Telegram-X | M7/Ff.java |
| https://foursquare.com/v/ | M7/Id.java |
| https://telegram.org/dlx | M7/Cif.java |
| https://telegram.org/dlx | M7/Hl.java |
| https://github.com/webmproject/libwebp.git/tree/845d5476a866141ba35ac133f856fa62f0b7445f | M7/Hl.java |
| https://github.com/FFmpeg/FFmpeg/tree/1606aab99bd84f0040fb0fa6ccccb092941f01ec | M7/Hl.java |
| https://github.com/TGX-Android/webrtc/tree/df2ed68b47022d4ab8c56f5fb6d8ec5a5bf4336d | M7/Hl.java |
| https://github.com/TGX-Android/tgcalls/tree/6adef64cda2255037d3d90a31753d1a9dd1abf39 | M7/Hl.java |
| https://play.google.com/store/apps/details?id=org.thunderdog.challegram | M7/Hl.java |
| https://play.google.com/store/apps/details?id=com.google.android.gms | M7/View$OnClickListenerC1750un.java |
| https://developer.android.com/reference/com/google/android/play/core/install/model/InstallErrorCode | H3/a.java |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | Q0/w.java |
| http://g.co/dev/packagevisibility. | Q0/C.java |
| https://telegram.org/dlx | R7/C2084n.java |
| https://play.google.com/store/apps/details?id=org.thunderdog.challegram | R7/C2084n.java |
| https://apps.samsung.com/appquery/appDetail.as?appId=org.thunderdog.challegram | R7/C2084n.java |
| https://appgallery.huawei.com/app/C101754199 | R7/C2084n.java |
| https://github.com/TGX-Android/Telegram-X/compare/22519922... | R7/C2084n.java |
| https://github.com/tdlib/td | R7/C2062c.java |
| https://github.com/TGX-Android/Telegram-X | R7/C2062c.java |
| http://telegra.ph/Telegram-X-03-26 | R7/AbstractC2093s.java |
| http://telegra.ph/Telegram-X-07-27 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-10-14 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-04-25 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-09-21 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-01-23-2 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-02-29 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-04-23 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-11-08 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-06-11 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-10-06 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-03-08 | R7/AbstractC2093s.java |
| https://t.me/tgx\_android/305 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-04-02 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-08-02 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-2023-12-31 | R7/AbstractC2093s.java |
| https://telegra.ph/Telegram-X-05-10 | R7/AbstractC2093s.java |
| https://firebaseappcheck.googleapis.com/v1/projects/%s/apps/%s:exchangePlayIntegrityToken?key=%s | T3/l.java |
| https://firebaseappcheck.googleapis.com/v1/projects/%s/apps/%s:exchangeDebugToken?key=%s | T3/l.java |
| https://firebaseappcheck.googleapis.com/v1/projects/%s/apps/%s:exchangeSafetyNetToken?key=%s | T3/l.java |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | V0/C2213f0.java |
| https://github.com/TGX-Android/Telegram-X/pull/602/files/9826472a455057a1ad35f1b4b236099cdef204b9 | W6/A.java |
| https://maps.googleapis.com/maps/api/staticmap?format=jpg&center=%f,%f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d&sensor=false%s | W6/L0.java |
| https://maps.googleapis.com/maps/api/staticmap?format=jpg&center=%f,%f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d&sensor=false&language=%s%s | W6/L0.java |
| https://issuetracker.google.com/issues/new?component=413107&template=1096568 | W1/C2306c.java |
| http://schemas.microsoft.com/DRM/2007/03/protocols/AcquireLicense | Y0/h0.java |
| https://x</LA\_URL> | Y0/g0.java |
| https://default.url | Y0/g0.java |
| https://plus.google.com/ | Y2/x0.java |
| https://firebase.google.com/support/privacy/init-options. | j4/C3749f.java |
| http://schemas.android.com/apk/res/android | n0/k.java |
| https://ss3.4sqi.net/img/categories\_v2/ | p7/X0.java |
| https://coub.com/embed/ | p7/C4656z.java |
| https://open.spotify.com/ | p7/C4656z.java |
| https://music.yandex.ru/iframe/ | p7/C4656z.java |
| https://t.me/ | p7/G7.java |
| https://telegram.org/embed | p7/C4528j0.java |
| http://xmlpull.org/v1/doc/features.html | r7/C4885y.java |
| https://issuetracker.google.com/issues/new?component=618491&template=1257717 | x/AbstractC5473h.java |
| http://ns.adobe.com/xap/1.0/ | p1/b.java |
| https://aomedia.org/emsg/ID3 | s1/C4890a.java |
| https://developer.apple.com/streaming/emsg-id3 | s1/C4890a.java |
| https://telegram.org/faq | 摸瓜V1引擎 |
| https://github.com/TGX-Android/Telegram-X/pull/297) | 摸瓜V1引擎 |
| https://t.me/tgx\_log | 摸瓜V1引擎 |
| https://github.com/tdlib/td/issues) | 摸瓜V1引擎 |
| https://t.me/tdlib\_bot) | 摸瓜V1引擎 |
| https://web.telegram.org/). | 摸瓜V1引擎 |
| https://github.com/tdlib/td/issues). | 摸瓜V1引擎 |
| https://support.google.com/googleplay/answer/9037938?hl=en | 摸瓜V1引擎 |
| https://firebaseinstallations.googleapis.com/ | 摸瓜V1引擎 |
| https://telegram.org/blog/coronavirus | 摸瓜V1引擎 |
| https://translations.telegram.org). | 摸瓜V1引擎 |
| https://translations.telegram.org/en/android\_x/), | 摸瓜V1引擎 |
| https://t.me/tgx\_android\_translate/) | 摸瓜V1引擎 |
| https://scenic-parity-125411.firebaseio.com | 摸瓜V1引擎 |
| https://play.google.com/apps/testing/org.thunderdog.challegram | 摸瓜V1引擎 |
| https://telegram.org/privacy | 摸瓜V1引擎 |
| https://ads.telegram.org | 摸瓜V1引擎 |
| https://translations.telegram.org/en/android\_x/unsorted/ | 摸瓜V1引擎 |
| https://github.com/tdlib/td/issues), | 摸瓜V1引擎 |
| https://github.com/tdlib/td/issues)- | 摸瓜V1引擎 |
| https://web.telegram.org/) | 摸瓜V1引擎 |
| https://t.me/tdlib\_bot), | 摸瓜V1引擎 |
| https://t.me/tgx\_logs | 摸瓜V1引擎 |
| https://web.telegram.org). | 摸瓜V1引擎 |
| https://t.me/tdlib\_bot)-botilla | 摸瓜V1引擎 |
| https://github.com/tdlib/td/issues); | 摸瓜V1引擎 |
| https://web.telegram.org/)). | 摸瓜V1引擎 |
| https://t.me/tgx\_log. | 摸瓜V1引擎 |
| https://web.telegram.org/), | 摸瓜V1引擎 |
| http://t.me/tgx\_log | 摸瓜V1引擎 |
| https://t.me/tgx\_logs | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-04-23 | 摸瓜V3引擎 |
| https://telegram.org/blog/coronavirus==This | 摸瓜V3引擎 |
| https://default.url | 摸瓜V3引擎 |
| firebaseinstallations.googleapis.com | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-06-11 | 摸瓜V3引擎 |
| https://developer.android.com/guide/topics/media/issues/player-accessed-on-wrong-thread | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-09-21 | 摸瓜V3引擎 |
| https://t.me/tgx\_logMQDet | 摸瓜V3引擎 |
| https://github.com/TGX-Android/Telegram-X | 摸瓜V3引擎 |
| http://t.me/tgx\_logCFA | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-03-08 | 摸瓜V3引擎 |
| googlehosted.l.googleusercontent.com | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-11-08 | 摸瓜V3引擎 |
| https://telegram.org/faq#troubleshooting). | 摸瓜V3引擎 |
| https://android.googlesource.com/toolchain/llvm-project | 摸瓜V3引擎 |
| https://t.me/ | 摸瓜V3引擎 |
| https://telegram.org/privacy | 摸瓜V3引擎 |
| http://telegra.ph/Telegram-X-07-27 | 摸瓜V3引擎 |
| https://developer.android.com/training/articles/direct-boot | 摸瓜V3引擎 |
| https://ss3.4sqi.net/img/categories\_v2/ | 摸瓜V3引擎 |
| https://github.com/TGX-Android/Telegram-X/pull/602/files/9826472a455057a1ad35f1b4b236099cdef204b9 | 摸瓜V3引擎 |
| https://web.telegram.org/)). | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-08-02 | 摸瓜V3引擎 |
| https://t.me/tgx\_android/305 | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android..org.thunderdog.challegram.v.CustomRecyclerView | 摸瓜V3引擎 |
| https://telegram.org/faq#general-questions | 摸瓜V3引擎 |
| https://telegram.org/dlx | 摸瓜V3引擎 |
| https://github.com/tdlib/td | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res-auto | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-10-06 | 摸瓜V3引擎 |
| https://t.me/tgx\_log==%1$s | 摸瓜V3引擎 |
| https://github.com/tdlib/td/issues)- | 摸瓜V3引擎 |
| https://telegram.org/faq#general-questions): | 摸瓜V3引擎 |
| https://t.me/tgx\_logL | 摸瓜V3引擎 |
| http://telegra.ph/Telegram-X-03-26 | 摸瓜V3引擎 |
| https://apps.samsung.com/appquery/appDetail.as?appId=org.thunderdog.challegram | 摸瓜V3引擎 |
| http://t.me/tgx\_log | 摸瓜V3引擎 |
| https://developer.android.com/guide/topics/media/issues/cleartext-not-permitted | 摸瓜V3引擎 |
| https://appgallery.huawei.com/app/C101754199 | 摸瓜V3引擎 |
| https://t.me/tdlib\_bot | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-05-10 | 摸瓜V3引擎 |
| lh3-dz.googleusercontent.com | 摸瓜V3引擎 |
| http://xmlpull.org/v1/doc/features.html#indent-output | 摸瓜V3引擎 |
| http://www.apache.org/licenses/LICENSE-2.0 | 摸瓜V3引擎 |
| https://translations.telegram.org/en/android\_x/ | 摸瓜V3引擎 |
| https://github.com/tdlib/td/issues); | 摸瓜V3引擎 |
| https://t.me/tdlib\_bot)-botilla | 摸瓜V3引擎 |
| https://telegram.org/faq#q-i-have-a-new-phone-number-what-do-i-do | 摸瓜V3引擎 |
| https://web.telegram.org/). | 摸瓜V3引擎 |
| http://schemas.android.com/apk/res/android | 摸瓜V3引擎 |
| https://scenic-parity-125411.firebaseio.com | 摸瓜V3引擎 |
| https://ads.telegram.org | 摸瓜V3引擎 |
| https://web.telegram.org). | 摸瓜V3引擎 |
| https://developer.android.com/reference/com/google/android/play/core/install/model/InstallErrorCode# | 摸瓜V3引擎 |
| https://telegram.org/embed | 摸瓜V3引擎 |
| https://translations.telegram.org). | 摸瓜V3引擎 |
| https://github.com/TGX-Android/Telegram-X/compare/22519922... | 摸瓜V3引擎 |
| https://telegram.org/privacy88https://translations.telegram.org/en/android\_x/unsorted/ | 摸瓜V3引擎 |
| https://github.com/tdlib/td/issues | 摸瓜V3引擎 |
| https://t.me/tgx\_log. | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-04-02 | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-2023-12-31 | 摸瓜V3引擎 |
| https://open.spotify.com/ | 摸瓜V3引擎 |
| https://t.me/tgx\_log$$This | 摸瓜V3引擎 |
| https://t.me/tgx\_logOREst | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-02-29 | 摸瓜V3引擎 |
| https://aomedia.org/emsg/ID3 | 摸瓜V3引擎 |
| http://g.co/dev/packagevisibility. | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-04-25 | 摸瓜V3引擎 |
| https://translations.telegram.org/en/android\_x/unsorted/ | 摸瓜V3引擎 |
| https://github.com/tdlib/td/issues). | 摸瓜V3引擎 |
| https://telegram.org/faq#general-questionsAAhttps://telegram.org/faq#q-i-have-a-new-phone-number-wha | 摸瓜V3引擎 |
| https://coub.com/embed/ | 摸瓜V3引擎 |
| https://t.me/tgx\_log | 摸瓜V3引擎 |
| https://web.telegram.org/ | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-01-23-2 | 摸瓜V3引擎 |
| https://t.me/tgx\_android\_translate/ | 摸瓜V3引擎 |
| https://t.me/tgx\_logeeVersi | 摸瓜V3引擎 |
| https://telegra.ph/Telegram-X-10-14 | 摸瓜V3引擎 |
| https://github.com/TGX-Android/Telegram-X/pull/297 | 摸瓜V3引擎 |
| https://telegram.org/blog/coronavirus44This | 摸瓜V3引擎 |
| https://t.me/tgx\_logdeDu | 摸瓜V3引擎 |
| https://telegram.org/blog/coronavirus | 摸瓜V3引擎 |
| https://www.google.com/v1/projects/reserve-5a846/databases/(default)/documents/ipconfig/v3 | lib/arm64-v8a/libtdjni.so |
| https://twitter.com/search?q= | lib/arm64-v8a/libtdjni.so |
| https://telegra.ph | lib/arm64-v8a/libtdjni.so |
| https://telesco.pe/ | lib/arm64-v8a/libtdjni.so |
| https://twitter.com/ | lib/arm64-v8a/libtdjni.so |
| https://t.me/ | lib/arm64-v8a/libtdjni.so |
| https://my.telegram.org | lib/arm64-v8a/libtdjni.so |
| https://twitter.com/hashtag/ | lib/arm64-v8a/libtdjni.so |
| https://reserve-5a846.firebaseio.com/ipconfigv3.json | lib/arm64-v8a/libtdjni.so |
| https://T.me/premiumbot?start=status | lib/arm64-v8a/libtdjni.so |
| https://www.instagram.com/explore/tags/ | lib/arm64-v8a/libtdjni.so |
| https://dns.google/resolve?name= | lib/arm64-v8a/libtdjni.so |
| https://www.instagram.com/ | lib/arm64-v8a/libtdjni.so |
| https://www.youtube.com/results?search\_query= | lib/arm64-v8a/libtdjni.so |
| https://software-download.microsoft.com/ | lib/arm64-v8a/libtdjni.so |
| https://music.youtube.com/search?q= | lib/arm64-v8a/libtdjni.so |
| https://firebaseremoteconfig.googleapis.com/v1/projects/peak-vista-421/namespaces/firebase:fetch?key=AIzaSyC2-kAkpDsroixRXw-sTw-Wfqo4NxjMwwM | lib/arm64-v8a/libtdjni.so |
| https://tgb-playground.smart-glocal.com/cds/v1/tokenize/card | lib/arm64-v8a/libtdjni.so |
| https://tgb.smart-glocal.com/cds/v1/tokenize/card | lib/arm64-v8a/libtdjni.so |
| https://crbug.com/1053756 | lib/arm64-v8a/libtgcallsjni.so |
| https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/, | lib/arm64-v8a/libtgcallsjni.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/arm64-v8a/libtgcallsjni.so |
| https://aomediacodec.github.io/av1-rtp-spec/ | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/arm64-v8a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/arm64-v8a/libtgcallsjni.so |
| https://www.google.com/v1/projects/reserve-5a846/databases/(default)/documents/ipconfig/v3 | lib/armeabi-v7a/libtdjni.so |
| https://twitter.com/search?q= | lib/armeabi-v7a/libtdjni.so |
| https://telegra.ph | lib/armeabi-v7a/libtdjni.so |
| https://telesco.pe/ | lib/armeabi-v7a/libtdjni.so |
| https://twitter.com/ | lib/armeabi-v7a/libtdjni.so |
| https://t.me/ | lib/armeabi-v7a/libtdjni.so |
| https://my.telegram.org | lib/armeabi-v7a/libtdjni.so |
| https://twitter.com/hashtag/ | lib/armeabi-v7a/libtdjni.so |
| https://reserve-5a846.firebaseio.com/ipconfigv3.json | lib/armeabi-v7a/libtdjni.so |
| https://T.me/premiumbot?start=status | lib/armeabi-v7a/libtdjni.so |
| https://www.instagram.com/explore/tags/ | lib/armeabi-v7a/libtdjni.so |
| https://dns.google/resolve?name= | lib/armeabi-v7a/libtdjni.so |
| https://www.instagram.com/ | lib/armeabi-v7a/libtdjni.so |
| https://www.youtube.com/results?search\_query= | lib/armeabi-v7a/libtdjni.so |
| https://software-download.microsoft.com/ | lib/armeabi-v7a/libtdjni.so |
| https://music.youtube.com/search?q= | lib/armeabi-v7a/libtdjni.so |
| https://firebaseremoteconfig.googleapis.com/v1/projects/peak-vista-421/namespaces/firebase:fetch?key=AIzaSyC2-kAkpDsroixRXw-sTw-Wfqo4NxjMwwM | lib/armeabi-v7a/libtdjni.so |
| https://tgb-playground.smart-glocal.com/cds/v1/tokenize/card | lib/armeabi-v7a/libtdjni.so |
| https://tgb.smart-glocal.com/cds/v1/tokenize/card | lib/armeabi-v7a/libtdjni.so |
| https://crbug.com/1053756 | lib/armeabi-v7a/libtgcallsjni.so |
| https://webrtc.googlesource.com/src/+/refs/heads/main/docs/native-code/rtp-hdrext/playout-delay/, | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.ietf.org/id/draft-holmer-rmcat-transport-wide-cc-extensions-01 | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-send-time | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/abs-capture-time | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-content-type | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-timing | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/generic-frame-descriptor-00 | lib/armeabi-v7a/libtgcallsjni.so |
| https://aomediacodec.github.io/av1-rtp-spec/ | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-layers-allocation00 | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/transport-wide-cc-02 | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/playout-delay | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/color-space | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/video-frame-tracking-id | lib/armeabi-v7a/libtgcallsjni.so |
| http://www.webrtc.org/experiments/rtp-hdrext/inband-cn | lib/armeabi-v7a/libtgcallsjni.so |

### **4.3 邮箱线索**

| 邮箱地址 | 所在文件 |
| --- | --- |
| u0013android@android.com0  u0013android@android.com | U2/A.java |
| tgx-android@pm.me  login@telegram.org  sms@telegram.org | 摸瓜V1引擎 |

### **4.4 手机号线索**

| 手机号 | 所在文件 |
| --- | --- |
| 15555215554 | j6/z.java |
| 15555215556 | j6/z.java |
| 15555215558 | j6/z.java |
| 15555215560 | j6/z.java |
| 15555215562 | j6/z.java |
| 15555215564 | j6/z.java |
| 15555215566 | j6/z.java |
| 15555215568 | j6/z.java |
| 15555215570 | j6/z.java |
| 15555215572 | j6/z.java |
| 15555215574 | j6/z.java |
| 15555215576 | j6/z.java |
| 15555215578 | j6/z.java |
| 15555215580 | j6/z.java |
| 15555215582 | j6/z.java |
| 15555215584 | j6/z.java |
| 14058229493 | lib/arm64-v8a/libtdjni.so |
| 14058229493 | lib/armeabi-v7a/libtdjni.so |

## **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: CN=Viacheslav Krylov 签名算法: rsassa\_pkcs1v15 有效期自: 2015-05-20 11:02:08+00:00 有效期至: 2040-05-13 11:02:08+00:00 发行人: CN=Viacheslav Krylov 序列号: 0x555c69b0 哈希算法: sha1 md5值: 7adfeafd11a4444f2c3cb7f668b9efca sha1值: 66462134345a6adac3c1d5aea9cef0421b7cab68 sha256值: eb801a303294ba02a84d030ebb1216c438ac985ad4b89208e32d7a7190dcdd33 sha512值: da0ba7243015ae88950fe7c18eafba241fc0468b407ba4cd93dd588b765ed6867262b27c9191464e98002c789976a7f73094e237e3b795637d14e7b75ff31391 公钥算法: rsa 密钥长度: 1024 指纹: d994b8f25611ef909eb743b6cefd27e3efb8e7fb068935454cedadcd0a1e0110**

## **6. 硬编码敏感信息**

| 可能的敏感信息 |
| --- |
| "AbortPassword" : "Abort Two-Step Verification Setup" |
| "ActivatingUsername" : "Activating username, please wait…" |
| "AreYouSureSessions" : "Are you sure you want to terminate all other sessions?" |
| "BlockUser" : "Block user" |
| "BlockedUser" : "%1$s has been blocked." |
| "BotUsername" : "Bot Link" |
| "CategoryArchivePrivate" : "Archive / Private" |
| "CategoryPrivate" : "Private" |
| "CategorySecret" : "Secret" |
| "ChangePassword" : "Change Password" |
| "ChannelPrivate" : "Private Channel" |
| "ChannelPrivateInfo" : "Private channels can only be joined via invite link." |
| "ChannelPrivateLinkHelp" : "People can join your channel by following this link. You can revoke the link at any time." |
| "ChannelRemoveUser" : "Remove from channel" |
| "ChatAccessPrivateChannel" : "This channel is private" |
| "ChatAccessPrivateGroup" : "This group is private" |
| "ChatWithUser" : "Chat with %1$s" |
| "ChooseYourPassword" : "Choose your password" |
| "ClearOtherSessionsHelp" : "Logs out all devices except for this one." |
| "ClearOtherWebSessionsHelp" : "You can log in on websites that support signing in with Telegram." |
| "CopiedLinkPrivate" : "Link has been copied to the clipboard. It works only for members of this chat." |
| "CopiedUsername" : "Username has been copied to the clipboard" |
| "CopyUsername" : "Copy username" |
| "DeactivatingUsername" : "Deactivating username, please wait…" |
| "DeleteForUser" : "Delete for %1$s" |
| "DeleteXForUser" : "" |
| "DisablePassword" : "Disable Password" |
| "EditBotUsername" : "Public Link" |
| "EditUsername" : "Edit Username" |
| "EncryptionKey" : "Encryption Key" |
| "EnterAPassword" : "Enter a password" |
| "EnterPassword" : "Enter Password" |
| "EraseDatabaseMultiUser" : "This action does not affect other accounts." |
| "GroupPrivate" : "Private Group" |
| "HideSecret" : "Hide on Lock Screen" |
| "InPrivateChats" : "In Private Chats" |
| "LeaveXPrivateChannel" : "" |
| "LeaveXPrivateChannel\_few" : "" |
| "LeaveXPrivateChannel\_many" : "" |
| "LeaveXPrivateChannel\_one" : "You will be unable to return to %1$s channel" |
| "LeaveXPrivateChannel\_other" : "You will be unable to return to %1$s channels" |
| "LeaveXPrivateChannel\_two" : "" |
| "LeaveXPrivateChannel\_zero" : "" |
| "LeaveXPrivateGroup" : "" |
| "LeaveXPrivateGroup\_few" : "" |
| "LeaveXPrivateGroup\_many" : "" |
| "LeaveXPrivateGroup\_one" : "You will be unable to return to %1$s group" |
| "LeaveXPrivateGroup\_other" : "You will be unable to return to %1$s groups" |
| "LeaveXPrivateGroup\_two" : "" |
| "LeaveXPrivateGroup\_zero" : "" |
| "LiveLocationAlertPrivate" : "Choose for how long %1$s will see your live location." |
| "LoadingUser" : "Loading user…" |
| "LoadingUsername" : "Loading username…" |
| "NoOtherSessions" : "No Other Active Sessions" |
| "NoOtherSessionsInfo" : "You can log in to Telegram from other mobile, tablet and desktop devices, using the same phone number. All your data will be instantly synchronized." |
| "NoPrivateChats" : "No private chats" |
| "NotificationChannelCommonPrivate" : "Default notification settings for all private chats and mentions." |
| "NotificationChannelUser" : "Custom notification settings for messages and mentions from %1$s." |
| "NotificationsPrivateInfo" : "You can set custom notifications for specific users on their profile page." |
| "OtherWebSessions" : "Connected Websites" |
| "PasscodeInvalidPassword" : "Invalid Password" |
| "PasscodeMismatchPassword" : "Passwords do not match" |
| "PrimaryUsername" : "Primary username" |
| "PrivacyActionUser" : "What is %1$s allowed to do?" |
| "PrivacyVisibilityUser" : "What can %1$s see on my profile?" |
| "PrivateChat" : "Private Chat" |
| "PrivateChats" : "Private Chats" |
| "PrivateChatsMentions" : "Private Chats and Mentions" |
| "ProxyCredentials" : "Credentials" |
| "ProxyCredentialsOptional" : "Credentials (optional)" |
| "QBlockUser" : "Block %1$s?" |
| "ReEnterAPassword" : "Re-enter a password" |
| "ReminderActionVerifyPassword" : "Verify Password" |
| "ReminderCheckTfaPassword" : "Check your password" |
| "ResetPassword" : "Reset password" |
| "RestrictUser" : "Restrict user" |
| "SecretChatWithUser" : "Secret chat with %1$s" |
| "SessionAccept" : "Accept" |
| "SessionAccepts" : "What can be received on this device?" |
| "SessionAcceptsCalls" : "Calls" |
| "SessionApp" : "Application" |
| "SessionAttempt" : "Login Attempt" |
| "SessionAttemptDetails" : "Login Attempt Details" |
| "SessionCalls" : "Incoming Calls" |
| "SessionDetails" : "Session Details" |
| "SessionDevice" : "Device" |
| "SessionFirstLogin" : "First Login" |
| "SessionIP" : "IP Address" |
| "SessionIpUnknown" : "Unknown" |
| "SessionLastActiveDate" : "Last active: %1$s" |
| "SessionLastLogin" : "Last Activity" |
| "SessionLocation" : "Location" |
| "SessionLocationUnknown" : "Unknown" |
| "SessionLogInDate" : "Logged in: %1$s" |
| "SessionReject" : "Reject" |
| "SessionSecretChats" : "Secret Chats" |
| "SessionSystem" : "System" |
| "SessionTerminateTtl" : "Terminate old sessions if inactive for" |
| "SessionTerminatesCustom" : "Enter custom value" |
| "SessionTerminatesCustomAlertTitle" : "Number of Days" |
| "SessionTerminatesInMonths" : "" |
| "SessionTerminatesInMonths\_few" : "" |
| "SessionTerminatesInMonths\_many" : "" |
| "SessionTerminatesInMonths\_one" : "Terminate in %1$s month" |
| "SessionTerminatesInMonths\_other" : "Terminate in %1$s months" |
| "SessionTerminatesInMonths\_two" : "" |
| "SessionTerminatesInMonths\_zero" : "" |
| "SessionTerminatesInWeeks" : "" |
| "SessionTerminatesInWeeks\_few" : "" |
| "SessionTerminatesInWeeks\_many" : "" |
| "SessionTerminatesInWeeks\_one" : "Terminate in %1$s week" |
| "SessionTerminatesInWeeks\_other" : "Terminate in %1$s weeks" |
| "SessionTerminatesInWeeks\_two" : "" |
| "SessionTerminatesInWeeks\_zero" : "" |
| "SessionUnknown" : "Unknown location" |
| "Sessions" : "Sessions" |
| "SessionsIncompleteInfo" : "The devices above have no access to your messages. The code was entered correctly, but no correct password was given." |
| "SessionsIncompleteTitle" : "Incomplete Login Attempts" |
| "SessionsTitle" : "Active Sessions" |
| "SetAdditionalPassword" : "Set additional password" |
| "SetUpUsername" : "Set Username" |
| "ShowSecret" : "Secret Chats on Lock Screen" |
| "SignedInNoOtherSessions" : "You have no other sessions" |
| "SignedInOtherSession" : "You are also signed in on %1$s" |
| "SuggestInvitingUser" : "%1$s is not on Telegram yet. Would you like to invite them via SMS?" |
| "TerminateAllSessions" : "Terminate All Other Sessions" |
| "TerminateAllWebSessions" : "Disconnect All Websites" |
| "TerminateIncompleteSession" : "Terminate login attempt" |
| "TerminateIncompleteSessionQuestion" : "Terminate this login attempt?" |
| "TerminateSession" : "Terminate session" |
| "TerminateSessionQuestion" : "Terminate this session?" |
| "TerminateWebSessionQuestion" : "Disconnect %1$s?" |
| "TransferOwnershipSecurityActionSetPassword" : "Set password" |
| "TransferOwnershipSecurityWaitPassword" : "Sorry, but you need to wait \*\*%1$s\*\* before you can transfer ownership, because you've set a password just recently." |
| "TransferOwnershipSecurityWaitSession" : "Sorry, but you need to wait \*\*%1$s\*\* before you can transfer ownership, because you've signed in on the current device just recently." |
| "UnblockedUser" : "%1$s has been unblocked." |
| "UnlockByPassword" : "Enter your password to unlock" |
| "UseProxyPassword" : "Password" |
| "UseProxyUsername" : "Username" |
| "Username" : "Username" |
| "WebSessionsTitle" : "Logged In with Telegram" |
| "YourPassword" : "Your Password" |
| "deletedUser" : "deleted user" |
| "firebase\_database\_url" : "https://scenic-parity-125411.firebaseio.com" |
| "format\_notificationScheduledPrivate" : "������ Scheduled message for %1$s" |
| "format\_sessionsAndWebsites" : "%1$s, %2$s" |
| "google\_api\_key" : "AIzaSyC\_eeOn-j16lB49kGu\_SnTujJwYNvMcWu4" |
| "google\_crash\_reporting\_api\_key" : "AIzaSyC\_eeOn-j16lB49kGu\_SnTujJwYNvMcWu4" |
| "login\_Password" : "Password" |
| "session\_App" : "App: %1$s" |
| "session\_Device" : "Device: %1$s" |
| "session\_LastActive" : "" |
| "session\_LastActive\_date" : "last active on %1$s at %2$s" |
| "session\_LastActive\_hours" : "" |
| "session\_LastActive\_hours\_few" : "" |
| "session\_LastActive\_hours\_many" : "" |
| "session\_LastActive\_hours\_one" : "last active %1$s hour ago" |
| "session\_LastActive\_hours\_other" : "last active %1$s hours ago" |
| "session\_LastActive\_hours\_two" : "" |
| "session\_LastActive\_hours\_zero" : "" |
| "session\_LastActive\_minutes" : "" |
| "session\_LastActive\_minutes\_few" : "" |
| "session\_LastActive\_minutes\_many" : "" |
| "session\_LastActive\_minutes\_one" : "last active %1$s minute ago" |
| "session\_LastActive\_minutes\_other" : "last active %1$s minutes ago" |
| "session\_LastActive\_minutes\_two" : "" |
| "session\_LastActive\_minutes\_zero" : "" |
| "session\_LastActive\_now" : "last active just now" |
| "session\_LastActive\_seconds" : "" |
| "session\_LastActive\_seconds\_few" : "" |
| "session\_LastActive\_seconds\_many" : "" |
| "session\_LastActive\_seconds\_one" : "last active %1$s second ago" |
| "session\_LastActive\_seconds\_other" : "last active %1$s seconds ago" |
| "session\_LastActive\_seconds\_two" : "" |
| "session\_LastActive\_seconds\_zero" : "" |
| "session\_LastActive\_today" : "last active at %1$s" |
| "session\_LastActive\_weekday" : "last active on %1$s at %2$s" |
| "session\_LastActive\_yesterday" : "last active yesterday at %1$s" |
| "session\_System" : "System: %1$s" |
| "session\_TerminatesIn" : "" |
| "session\_TerminatesIn\_date" : "auto-terminates on %1$s at %2$s" |
| "session\_TerminatesIn\_hours" : "" |
| "session\_TerminatesIn\_hours\_few" : "" |
| "session\_TerminatesIn\_hours\_many" : "" |
| "session\_TerminatesIn\_hours\_one" : "auto-terminates within %1$s hour" |
| "session\_TerminatesIn\_hours\_other" : "auto-terminates within %1$s hours" |
| "session\_TerminatesIn\_hours\_two" : "" |
| "session\_TerminatesIn\_hours\_zero" : "" |
| "session\_TerminatesIn\_minutes" : "" |
| "session\_TerminatesIn\_minutes\_few" : "" |
| "session\_TerminatesIn\_minutes\_many" : "" |
| "session\_TerminatesIn\_minutes\_one" : "auto-terminates within %1$s minute" |
| "session\_TerminatesIn\_minutes\_other" : "auto-terminates within %1$s minutes" |
| "session\_TerminatesIn\_minutes\_two" : "" |
| "session\_TerminatesIn\_minutes\_zero" : "" |
| "session\_TerminatesIn\_now" : "auto-terminating now" |
| "session\_TerminatesIn\_seconds" : "" |
| "session\_TerminatesIn\_seconds\_few" : "" |
| "session\_TerminatesIn\_seconds\_many" : "" |
| "session\_TerminatesIn\_seconds\_one" : "auto-terminates within %1$s second" |
| "session\_TerminatesIn\_seconds\_other" : "auto-terminates within %1$s seconds" |
| "session\_TerminatesIn\_seconds\_two" : "" |
| "session\_TerminatesIn\_seconds\_zero" : "" |
| "session\_TerminatesIn\_today" : "auto-terminates at %1$s" |
| "session\_TerminatesIn\_tomorrow" : "auto-terminates tomorrow at %1$s" |
| "session\_TerminatesIn\_weekday" : "auto-terminates on %1$s at %2$s" |
| "unknownUser" : "unknown user" |
| "xRepliesToUser" : "" |
| "xSessions" : "" |
| "xSessions\_few" : "" |
| "xSessions\_many" : "" |
| "xSessions\_one" : "%1$s session" |
| "xSessions\_other" : "%1$s sessions" |
| "xSessions\_two" : "" |
| "xSessions\_zero" : "" |
| "ProxyCredentials" : "Credencials" |
| "ProxyCredentialsOptional" : "Credencials (opcional)" |
| "ProxyCredentials" : "مدارک" |
| "ProxyCredentialsOptional" : "مدارک (اختیاری)" |
| "ProxyCredentials" : "சான்றுகள்" |
| "ProxyCredentialsOptional" : "சான்றுகள் (விரும்பினால்)" |
| "ProxyCredentials" : "Legitimasjon" |
| "ProxyCredentialsOptional" : "Legitimasjon (valgfritt)" |
| "ProxyCredentials" : "Уліковыя даныя" |
| "ProxyCredentialsOptional" : "Уліковыя даныя (неабавязкова)" |
| "ProxyCredentials" : "Zugangsdaten" |
| "ProxyCredentialsOptional" : "Zugangsdaten (optional)" |
| "ProxyCredentials" : "אישורי אבטחה" |
| "ProxyCredentialsOptional" : "אישורי אבטחה (רשות)" |
| "ProxyCredentials" : "Pääsytiedot" |
| "ProxyCredentialsOptional" : "Pääsytiedot (valinnainen)" |
| "ProxyCredentials" : "Растаушы" |
| "ProxyCredentialsOptional" : "РАСТАУШЫ (МІНДЕТТІ ЕМЕС)" |
| "ProxyCredentials" : "Prihlasovacie údaje" |
| "ProxyCredentialsOptional" : "Prihlasovacie údaje (voliteľné)" |
| "ProxyCredentials" : "Облікові дані" |
| "ProxyCredentialsOptional" : "Облікові дані (необовʼязково)" |
| "ProxyCredentials" : "ക്രെഡൻഷ്യലുകൾ" |
| "ProxyCredentialsOptional" : "ക്രെഡൻഷ്യലുകൾ (നിര്‍ബന്ധമല്ലാത്ത)" |
| "ProxyCredentials" : "Dane uwierzytelniające" |
| "ProxyCredentialsOptional" : "Dane uwierzytelniające (opcjonalnie)" |
| "ProxyCredentials" : "Identigiloj" |
| "ProxyCredentialsOptional" : "Identigiloj (nedevigaj)" |
| "ProxyCredentials" : "Credențiale" |
| "ProxyCredentialsOptional" : "Acreditare (optională)" |
| "ProxyCredentials" : "الشهادات" |
| "ProxyCredentialsOptional" : "الشهادات (اختياري)" |
| "ProxyCredentials" : "Identifiants" |
| "ProxyCredentialsOptional" : "Identifiants (optionnels)" |
| "ProxyCredentials" : "Ovlaštenja" |
| "ProxyCredentialsOptional" : "Ovlaštenje (neobavezno)" |
| "ProxyCredentials" : "Акредитиви" |
| "ProxyCredentialsOptional" : "Акредитиви (необавезно)" |
| "ProxyCredentials" : "Kimlik bilgileri" |
| "ProxyCredentialsOptional" : "Kimlik bilgileri (isteğe bağlı)" |
| "ProxyCredentials" : "Přihlašovací údaje" |
| "ProxyCredentialsOptional" : "Přihlašovací údaje (volitelné)" |
| "ProxyCredentials" : "Credenciales" |
| "ProxyCredentialsOptional" : "Credenciales (opcional)" |
| "ProxyCredentials" : "Kelayakan" |
| "ProxyCredentialsOptional" : "Kelayakan (opsyen)" |
| "ProxyCredentials" : "Credenziali" |
| "ProxyCredentialsOptional" : "Credenziali (opzionali)" |
| "ProxyCredentials" : "Hitelesítés" |
| "ProxyCredentialsOptional" : "Hitelesítő adatok (opcionális)" |
| "ProxyCredentials" : "Учётные данные" |
| "ProxyCredentialsOptional" : "Учётные данные (необязательно)" |
| "ProxyCredentials" : "Referenser" |
| "ProxyCredentialsOptional" : "Referenser (frivilligt)" |
| "ProxyCredentials" : "אישורי אבטחה" |
| "ProxyCredentialsOptional" : "אישורי אבטחה (רשות)" |
| "ProxyCredentials" : "Credenciais" |
| "ProxyCredentialsOptional" : "Credenciais (opcional)" |

## **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.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.FLASHLIGHT | 正常 | 控制手电筒 | 允许应用程序控制手电筒 |
| android.permission.INTERNET | 正常 | 互联网接入 | 允许应用程序创建网络套接字 |
| android.permission.ACCESS\_NETWORK\_STATE | 正常 | 查看网络状态 | 允许应用程序查看所有网络的状态 |
| android.permission.ACCESS\_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.ACCESS\_COARSE\_LOCATION | 危险 | 粗定位 | 访问粗略位置源,例如移动网络数据库,以确定大概的电话位置（如果可用）。恶意应用程序可以使用它来确定您的大致位置 |
| android.permission.ACCESS\_BACKGROUND\_LOCATION | 危险 | 后台访问位置 | 允许应用程序在后台访问位置 |
| 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 |
| android.permission.RECORD\_AUDIO | 危险 | 录音 | 允许应用程序访问音频记录路径 |
| android.permission.MODIFY\_AUDIO\_SETTINGS | 正常 | 更改您的音频设置 | 允许应用程序修改全局音频设置,例如音量和路由 |
| 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 |
| android.permission.VIBRATE | 正常 | 可控震源 | 允许应用程序控制振动器 |
| 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.USE\_FINGERPRINT | 正常 | allow use of指纹 | 该常量在 API 级别 28 中已被弃用。应用程序应改为请求 USE\_BIOMETRIC |
| android.permission.FOREGROUND\_SERVICE | 正常 |  | 允许常规应用程序使用 Service.startForeground。 |
| android.permission.FOREGROUND\_SERVICE\_LOCATION | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_MEDIA\_PLAYBACK | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.FOREGROUND\_SERVICE\_PHONE\_CALL | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.MANAGE\_OWN\_CALLS | 正常 |  | 允许调用应用程序通过自我管理的 ConnectionService API 管理自己的调用 |
| android.permission.CHANGE\_CONFIGURATION | 系统需要 | 更改您的 UI 设置 | 允许应用程序更改当前配置,例如语言环境或整体字体大小 |
| 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.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.SYSTEM\_ALERT\_WINDOW | 危险 | 显示系统级警报 | 允许应用程序显示系统警报窗口。恶意应用程序可以接管手机的整个屏幕 |
| android.permission.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.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.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.POST\_NOTIFICATIONS | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_IMAGES | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_VIDEO | 未知 | Unknown permission | Unknown permission from android reference |
| android.permission.READ\_MEDIA\_AUDIO | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.providers.gsf.permission.READ\_GSERVICES | 未知 | Unknown permission | Unknown permission from android reference |
| com.google.android.c2dm.permission.RECEIVE | 合法 | C2DM 权限 | 云到设备消息传递的权限 |
| org.thunderdog.challegram.permission.MAPS\_RECEIVE | 未知 | Unknown permission | Unknown permission from android reference |
| org.thunderdog.challegram.permission.C2D\_MESSAGE | 未知 | Unknown permission | Unknown permission from android reference |
| com.sec.android.provider.badge.permission.READ | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sec.android.provider.badge.permission.WRITE | 正常 | 在应用程序上显示通知计数 | 在三星手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.htc.launcher.permission.UPDATE\_SHORTCUT | 正常 | 在应用程序上显示通知计数 | 在 htc 手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonyericsson.home.permission.BROADCAST\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.sonymobile.home.permission.PROVIDER\_INSERT\_BADGE | 正常 | 在应用程序上显示通知计数 | 在索尼手机的应用程序启动图标上显示通知计数或徽章。 |
| com.anddoes.launcher.permission.UPDATE\_COUNT | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或徽章 |
| com.majeur.launcher.permission.UPDATE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在应用程序启动图标上显示通知计数或标记为固体。 |
| com.huawei.android.launcher.permission.CHANGE\_BADGE | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章。 |
| com.huawei.android.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| com.huawei.android.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在华为手机的应用程序启动图标上显示通知计数或徽章 |
| android.permission.READ\_APP\_BADGE | 正常 | 显示应用程序通知 | 允许应用程序显示应用程序图标徽章 |
| com.oppo.launcher.permission.READ\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| com.oppo.launcher.permission.WRITE\_SETTINGS | 正常 | 在应用程序上显示通知计数 | 在oppo手机的应用程序启动图标上显示通知计数或徽章。 |
| android.permission.READ\_SYNC\_SETTINGS | 正常 | 读取同步设置 | 允许应用程序读取同步设置,例如是否为联系人启用同步 |
| android.permission.WRITE\_SYNC\_SETTINGS | 正常 | 写入同步设置 | 允许应用程序修改同步设置,例如是否为联系人启用同步 |
| android.permission.GET\_ACCOUNTS | 危险 | 列出帐户 | 允许访问账户服务中的账户列表 |
| android.permission.AUTHENTICATE\_ACCOUNTS | 危险 | 充当帐户验证器 | 允许应用程序使用帐户管理器的帐户验证器功能,包括创建帐户以及获取和设置其密码 |
| org.thunderdog.challegram.DYNAMIC\_RECEIVER\_NOT\_EXPORTED\_PERMISSION | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_READ | 未知 | Unknown permission | Unknown permission from android reference |
| me.everything.badger.permission.BADGE\_COUNT\_WRITE | 未知 | Unknown permission | Unknown permission from android reference |

## **10. 应用内通信**

| 活动(ACTIVITY) | 通信(INTENT) |
| --- | --- |
| org.thunderdog.challegram.MainActivity | **Schemes**: http://, https://, tg://,  **Hosts:** t.me, tx.me, telegram.me, telegram.dog,  **Mime Types:** text/plain, image/\*, video/\*, \*/\*, |

**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。**