



Telegram 11.14.1.APK 分析报告



APP名称:	Telegram
包名:	org.telegram.messenger
域名线索:	35条
URL线索:	56条
邮箱线索:	3条

分析日期:2025年9月1日

分析平台:[摸瓜APK反编译平台](#)

文件信息

文件名: Telegram_11.14.1_APkPure.xapk
文件大小: 25.35MB
MD5值: fc16d865205e0b0c7fb0fd6cceda4820
SHA1值: 3a01db53025f7893da38ba041ea5027ab3beea8f
SHA256值: b0ce6bfef1cdc70b7881d993f69563d742277495c97e86e23785c100176083d4

APP 信息

App名称: Telegram
包名: org.telegram.messenger
主活动Activity: org.telegram.ui.LaunchActivity
安卓版本名称: 11.14.1
安卓版本: 61082

域名线索

域名	服务器信息
coub.com	IP: 95.213.253.85 所属国家: Russian Federation 地区: Sankt-Peterburg 城市: Saint Petersburg

	纬度: 59.894440 经度: 30.264200
youtube.googleapis.com	IP: 142.251.33.74 所属国家: Canada 地区: Ontario 城市: Toronto 纬度: 43.653660 经度: -79.382927
static-maps.yandex.ru	IP: 213.180.204.41 所属国家: Russian Federation 地区: Moskva 城市: Moscow 纬度: 55.752258 经度: 37.615471
api.twitch.tv	IP: 23.234.30.58 所属国家: United States of America 地区: Delaware 城市: Newark 纬度: 39.707489 经度: -75.734329
fragment.com	IP: 172.66.170.24 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
appgallery.huawei.com	IP: 121.36.119.11 所属国家: China 地区: Beijing 城市: Beijing 纬度: 39.907501 经度: 116.397102
tgb-playground.smart-glocal.com	IP: 99.83.179.90 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
dns.google.com	IP: 8.8.8.8 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
telegram.org	IP: 0.0.0.0 所属国家: - 地区: -

	城市: - 纬度: 0.000000 经度: 0.000000
maps.googleapis.com	IP: 142.251.215.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.instagram.com	IP: 104.244.45.246 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
www.aparat.com	IP: 185.147.178.13 所属国家: Iran (Islamic Republic of) 地区: Tehran 城市: Tehran 纬度: 35.694241 经度: 51.421310
t.me	IP: 0.0.0.0 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000
tgb.smart-glocal.com	IP: 75.2.95.23 所属国家: United States of America 地区: Washington 城市: Seattle 纬度: 47.604309 经度: -122.329842
maps.googleapis	没有服务器地理信息.
www.example.com	IP: 88.221.83.146 所属国家: Belgium 地区: Brussels Hoofdstedelijk Gewest 城市: Brussels 纬度: 50.850849 经度: 4.348780
attheme.org	IP: 127.0.0.1 所属国家: - 地区: - 城市: - 纬度: 0.000000 经度: 0.000000

schema.org	IP: 142.250.73.110 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
www.google.com	IP: 199.59.148.229 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
promote.telegram.org	IP: 202.182.98.125 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
ss3.4sqi.net	IP: 151.101.90.132 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
mozilla.cloudflare-dns.com	IP: 162.159.61.4 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
player.vimeo.com	IP: 199.16.158.8 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.773968 经度: -122.410446
instagram.com	IP: 67.228.235.93 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958
translate.googleapis.com	IP: 142.251.215.234 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514

maps.google.com	IP: 142.250.73.78 所属国家: United States of America 地区: California 城市: Mountain View 纬度: 37.405991 经度: -122.078514
stripe.com	IP: 18.140.144.179 所属国家: Singapore 地区: Singapore 城市: Singapore 纬度: 1.289987 经度: 103.850281
www.youtube.com	IP: 31.13.94.49 所属国家: Argentina 地区: Ciudad Autonoma de Buenos Aires 城市: Buenos Aires 纬度: -34.603600 经度: -58.381554
messenger.telegram.org	IP: 54.89.135.129 所属国家: United States of America 地区: Virginia 城市: Ashburn 纬度: 39.039474 经度: -77.491806
api.stripe.com	IP: 13.230.90.110 所属国家: Japan 地区: Tokyo 城市: Tokyo 纬度: 35.689499 经度: 139.692322
play.google.com	IP: 93.46.8.90 所属国家: Italy 地区: Lombardia 城市: Milan 纬度: 45.464336 经度: 9.188547
tonviewer.com	IP: 104.26.7.189 所属国家: United States of America 地区: California 城市: San Francisco 纬度: 37.775700 经度: -122.395203
youtube.com	IP: 31.13.88.169 所属国家: Ireland 地区: Dublin 城市: Dublin 纬度: 53.344151 经度: -6.267249

twitter.com	IP: 115.126.100.160 所属国家: Hong Kong 地区: Hong Kong 城市: Hong Kong 纬度: 22.285521 经度: 114.157692
usher.ttvnw.net	IP: 18.244.214.13 所属国家: United States of America 地区: California 城市: San Jose 纬度: 37.339390 经度: -121.894958

🌐 URL线索

URL信息	Url所在文件
https://maps.googleapis.com/maps/api/staticmap?center=%6f,%6f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d&markers=color:red%7Csize:mid%7C%6f,%6f&sensor=false&key=%s	org/telegram/messenger/AndroidUtilities.java
https://maps.googleapis.com/maps/api/staticmap?center=%6f,%6f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d&key=%s	org/telegram/messenger/AndroidUtilities.java
https://maps.googleapis.com/maps/api/staticmap?center=%6f,%6f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d&markers=color:red%7Csize:mid%7C%6f,%6f&sensor=false	org/telegram/messenger/AndroidUtilities.java
https://maps.googleapis.com/maps/api/staticmap?center=%6f,%6f&zoom=%d&size=%dx%d&maptype=roadmap&scale=%d	org/telegram/messenger/AndroidUtilities.java
https://static-maps.yandex.ru/1.x/?ll=%6f,%6f&z=%d&size=%d,%d&l=map&scale=%d&pt=%6f,%6f,vkbkm&lang=%s	org/telegram/messenger/AndroidUtilities.java
https://static-maps.yandex.ru/1.x/?ll=%6f,%6f&z=%d&size=%d,%d&l=map&scale=%d&lang=%s	org/telegram/messenger/AndroidUtilities.java
https://t.me/+PublicChat	org/telegram/messenger/MessageObject.java
https://instagram.com/	org/telegram/messenger/MessageObject.java
https://www.instagram.com/explore/tags/	org/telegram/messenger/MessageObject.java
https://twitter.com/	org/telegram/messenger/MessageObject.java
https://twitter.com/hashtag/	org/telegram/messenger/MessageObject.java
https://ss3.4sqi.net/img/categories_v2/building/government_capitolbuilding_64.png	org/telegram/messenger/LocationController.java
https://ss3.4sqi.net/img/categories_v2/travel/hotel_64.png	org/telegram/messenger/LocationController.java

https://play.google.com/store/apps/details?id=org.telegram.messenger	org/telegram/messenger/BuildVars.java
https://appgallery.huawei.com/app/C101184875	org/telegram/messenger/BuildVars.java
https://telegram.org/dl	org/telegram/messenger/ContactsController.java
https://play.google.com/store/account/subscriptions?sku=%s&package=%s	org/telegram/messenger/BillingController.java
https://static-maps	org/telegram/messenger/ImageLoader.java
https://maps.googleapis	org/telegram/messenger/ImageLoader.java
https://tonviewer.com/	org/telegram/messenger/MessagesController.java
https://t.me/premiumbot?start=status	org/telegram/messenger/MessagesController.java
https://play.google.com/store/account/subscriptions?sku=telegram_premium&package=org.telegram.messenger	org/telegram/messenger/MessagesController.java
https://telegram.org/	org/telegram/messenger/MessagesController.java
https://telegram.org/blog/telegram-stars	org/telegram/messenger/AppGlobalConfig.java
https://t.me/proxy?	org/telegram/messenger/SharedConfig.java
https://t.me/socks?	org/telegram/messenger/SharedConfig.java
http://t.me/	org/telegram/messenger/browser/Browser.java
https://t.me/	org/telegram/messenger/browser/Browser.java
http://www.google.com	org/telegram/messenger/browser/Browser.java
https://)?t\\.me/iv\\??(/.*	org/telegram/messenger/browser/Browser.java
https://)?telegram\\.org/(blog	org/telegram/messenger/browser/Browser.java
https://)?fragment\\.com(/.*	org/telegram/messenger/browser/Browser.java
https://t.me/call/	org/telegram/messenger/voip/VoIPService.java
http://www.example.com	org/telegram/messenger/support/customtabsclient/shared/CustomTabsHelper.java
https://t\\.me/(\\w+)?/(\\d+))?	org/telegram/ui/ChatActivity.java
https://t.me/	org/telegram/ui/ChatActivity.java
https://fragment.com/username/	org/telegram/ui/ChatActivity.java

https://)?t.me/([0-9a-zA-Z_]+)/([0-9]+)/?([0-9]+)?	org/telegram/ui/ChatActivity.java
https://)?t.me/([0-9a-zA-Z_]+)\{voicechat+	org/telegram/ui/ChatActivity.java
https://)?t.me/c/([0-9]+)/([0-9]+)/?([0-9]+)?	org/telegram/ui/ChatActivity.java
https://play.google.com/store/apps/details?id=com.google.android.webview	org/telegram/ui/PaymentFormActivity.java
https://tgb-playground.smart-glocal.com/cds/v1/tokenize/card	org/telegram/ui/PaymentFormActivity.java
https://tgb.smart-glocal.com/cds/v1/tokenize/card	org/telegram/ui/PaymentFormActivity.java
https://t.me/socks?	org/telegram/ui/ProxySettingsActivity.java
https://t.me/proxy?	org/telegram/ui/ProxySettingsActivity.java
https://t.me/+%	org/telegram/ui/PrivacyControlActivity.java
https://t.me/	org/telegram/ui/PremiumPreviewFragment.java
https://t.me/\$	org/telegram/ui/PremiumPreviewFragment.java
https://t.me/	org/telegram/ui/LaunchActivity.java
http://schema.org/CompletedActionStatus	org/telegram/ui/LaunchActivity.java
http://schema.org/FailedActionStatus	org/telegram/ui/LaunchActivity.java
https://t.me/BotFather?start=	org/telegram/ui/ChatEditActivity.java
https://t.me/BotFather	org/telegram/ui/ChatEditActivity.java
https://fragment.com	org/telegram/ui/ProfileActivity.java
http://maps.google.com/maps	org/telegram/ui/ProfileActivity.java
https://t.me/	org/telegram/ui/PhotoViewer.java
https://play.google.com/store/apps/details?id=com.google.android.webview	org/telegram/ui/ArticleViewer.java
https://telegram.org/embed	org/telegram/ui/ArticleViewer.java
https://fragment.com/username/	org/telegram/ui/ChatEditTypeActivity.java
https://ss3.4sqi.net/img/categories_v2/	org/telegram/ui/LocationActivity.java
http://maps.google.com/maps	org/telegram/ui/LocationActivity.java

https://fragment.com/username/	org/telegram/ui/ChangeUsernameActivity.java
https://fragment.com	org/telegram/ui/ChangeUsernameActivity.java
https://telegram.org/deactivate?phone=	org/telegram/ui/PassportActivity.java
https://promote.telegram.org/guidelines	org/telegram/ui/ReportBottomSheet.java
https://fragment.com/username/	org/telegram/ui/ChannelCreateActivity.java
https://telegram.org	org/telegram/ui/ThemePreviewActivity.java
https://t.me/+	org/telegram/ui/ManageLinksActivity.java
https://t.me/joinchat/	org/telegram/ui/ManageLinksActivity.java
https://t.me/	org/telegram/ui/ManageLinksActivity.java
https://telegram.org/	org/telegram/ui/Cells/ThemePreviewMessagesCell.java
https://telegram.org	org/telegram/ui/Cells/ThemePreviewMessagesCell.java
https://t.me/m/	org/telegram/ui/Business/BusinessLinksController.java
https://attheme.org?slug=	org/telegram/ui/ActionBar/Theme.java
https://t.me/	org/telegram/ui/Components/PermanentLinkBottomSheet.java
https://t.me/	org/telegram/ui/Components/DialogsBotsAdapter.java
https://play.google.com/store/apps/details?id=com.google.android.webview	org/telegram/ui/Components/EmbedBottomSheet.java
https://www.youtube.com/iframe_api\	org/telegram/ui/Components/EmbedBottomSheet.java
https://messenger.telegram.org/	org/telegram/ui/Components/EmbedBottomSheet.java
https://youtube.com	org/telegram/ui/Components/EmbedBottomSheet.java
https://t.me/	org/telegram/ui/Components/URLSpanNoUnderline.java
https://translate.googleapis.com/transl	org/telegram/ui/Components/TranslateAlert2.java
https://t.me/	org/telegram/ui/Components/TranslateAlert2.java
https://www.youtube.com/watch?v=	org/telegram/ui/Components/PhotoViewerWebView.java
https://www.youtube.com/youtubei/v1/player?key=	org/telegram/ui/Components/PhotoViewerWebView.java

https://messenger.telegram.org/	org/telegram/ui/Components/PhotoViewerWebView.java
https://youtube.com	org/telegram/ui/Components/PhotoViewerWebView.java
http://www.aparat.com/video/video/embed/vt/frame/showvideo/yes/videohash/%s	org/telegram/ui/Components/WebPlayerView.java
https://coub.com/api/v2/coubs/%s.json	org/telegram/ui/Components/WebPlayerView.java
https://api.twitch.tv/kraken/streams/%s?stream_type=all	org/telegram/ui/Components/WebPlayerView.java
https://api.twitch.tv/api/channels/%s/access_token	org/telegram/ui/Components/WebPlayerView.java
https://youtube.googleapis.com/v/	org/telegram/ui/Components/WebPlayerView.java
https://usher.ttvnw.net/api/channel/hls/%s.m3u8?%s	org/telegram/ui/Components/WebPlayerView.java
https://player.vimeo.com/video/%s/config	org/telegram/ui/Components/WebPlayerView.java
https://www.youtube.com/embed/	org/telegram/ui/Components/WebPlayerView.java
https://www.youtube.com/get_video_info?	org/telegram/ui/Components/WebPlayerView.java
https://www.youtube.com	org/telegram/ui/Components/WebPlayerView.java
https://ss3.4sqi.net/img/categories_v2/	org/telegram/ui/Components/ChatAttachAlertLocationLayout.java
https://play.google.com/store/apps/details?id=org.telegram.messenger	org/telegram/ui/Components/Premium/PremiumNotAvailableBottomSheet.java
https://t.me/giftcode/	org/telegram/ui/Components/Premium/boosts/PremiumPreviewGiftLinkBottomSheet.java
https://t.me/giftcode/	org/telegram/ui/Components/Premium/boosts/cells/LinkCell.java
https://t.me/giftcode/	org/telegram/ui/Components/Premium/boosts/adapters/GiftInfoAdapter.java
https://t.me/stickers	org/telegram/ui/Components/Reactions/ChatCustomReactionsEditActivity.java
https://t.me/nft/	org/telegram/ui/Stars/ProfileGiftsView.java
https://t.me/\$	org/telegram/ui/Stars/StarsIntroActivity.java
https://t.me/boost/?c=	org/telegram/ui/Stories/ChannelBoostUtilities.java
https://t.me/boost/	org/telegram/ui/Stories/ChannelBoostUtilities.java
https://t.me/%1\$s/s/%2\$s	org/telegram/ui/Stories/PeerStoriesView.java
https://play.google.com/store/apps/details?id=com.google.android.webview	org/telegram/ui/web/BotWebViewContainer.java

https://t.me/	org/telegram/ui/web/BotWebViewContainer.java
https://ss3.4sqi.net/img/categories_v2/travel/hotel_64.png	org/telegram/ui/Adapters/BaseLocationAdapter.java
https://ss3.4sqi.net/img/categories_v2/building/government_capitolbuilding_64.png	org/telegram/ui/Adapters/BaseLocationAdapter.java
https://ss3.4sqi.net/img/categories_v2/	org/telegram/ui/Adapters/BaseLocationAdapter.java
https://dns.google.com/resolve?name=	org/telegram/tgnet/ConnectionsManager.java
https://mozilla.cloudflare-dns.com/dns-query?name=	org/telegram/tgnet/ConnectionsManager.java
https://www.google.com/resolve?name=	org/telegram/tgnet/ConnectionsManager.java
https://stripe.com/docs/stripe.js.	com/stripe/android/Stripe.java
https://stripe.com/docs/stripe.js	com/stripe/android/Stripe.java
https://api.stripe.com	com/stripe/android/net/StripeApiHandler.java
https://twitter.com/stripestatus,	com/stripe/android/net/StripeApiHandler.java
https://stripe.com/api	com/stripe/android/net/StripeApiHandler.java

 邮箱线索

邮箱地址	所在文件
sms@telegram.org	org/telegram/ui/PassportActivity.java
sms@telegram.org recover@telegram.org login@stel.com	org/telegram/ui/LoginActivity.java
support@stripe.com	com/stripe/android/net/StripeApiHandler.java

 手机线索

手机号	所在文件
1522222222	org/telegram/messenger/MessageObject.java
1922222222	org/telegram/messenger/MessagesStorage.java

15555215554	org/telegram/messenger/EmuDetector.java
15555215556	org/telegram/messenger/EmuDetector.java
15555215558	org/telegram/messenger/EmuDetector.java
15555215560	org/telegram/messenger/EmuDetector.java
15555215562	org/telegram/messenger/EmuDetector.java
15555215564	org/telegram/messenger/EmuDetector.java
15555215566	org/telegram/messenger/EmuDetector.java
15555215568	org/telegram/messenger/EmuDetector.java
15555215570	org/telegram/messenger/EmuDetector.java
15555215572	org/telegram/messenger/EmuDetector.java
15555215574	org/telegram/messenger/EmuDetector.java
15555215576	org/telegram/messenger/EmuDetector.java
15555215578	org/telegram/messenger/EmuDetector.java
15555215580	org/telegram/messenger/EmuDetector.java
15555215582	org/telegram/messenger/EmuDetector.java
15555215584	org/telegram/messenger/EmuDetector.java
1322222222	org/telegram/messenger/SendMessagesHelper.java
1622222222	org/telegram/messenger/SendMessagesHelper.java
1822222222	org/telegram/messenger/SendMessagesHelper.java
1522222222	org/telegram/ui/Cells/ChatMessageCell.java
1322222222	org/telegram/ui/Cells/ChatMessageCell.java
1622222222	org/telegram/ui/Stars/StarsIntroActivity.java

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: L=Saint-Petersburg, O=VK, OU=VK, CN=Nikolay Kudashov
签名算法: rsassa_pkcs1v15
有效期自: 2013-08-29 19:13:13+00:00
有效期至: 2038-08-23 19:13:13+00:00
发行人: L=Saint-Petersburg, O=VK, OU=VK, CN=Nikolay Kudashov
序列号: 0x521f9d49
哈希算法: sha1
md5值: 26bab62540ef0c20bfc6bacf3d3b1f5
sha1值: 9723e5838612e9c7c08ca2c6573b6026d7a51f8f
sha256值: 49c1522548ebacd46ce322b6fd47f6092bb745d0f88082145caf35e14dcc38e1
sha512值: b47593b965b36396b06296546de386e452f84180968bca894ac90c5dfdbdedae97c3701f0454ec90f1a616e0bb5ab2c8b4bd8efdbd7b8649268fc7b1f614d648
公钥算法: rsa
密钥长度: 1024
指纹: 5a75db88b7dde612c71b129469a376894dee2c4d8c3266380b658d837ee46677

硬编码敏感信息

加壳分析

加壳类型	所属文件
登陆摸瓜网站后查看	

第三方插件

名称	分类	URL链接
登陆摸瓜网站后查看		

此APP的危险动作

应用内通信