RKS Global

rks.global

Testing Alternative Telegram Clients

Analysis of 8 alternative Telegram clients for Android for evidence of data transmission to Russian infrastructure and the presence of hidden surveillance mechanisms

Table of contents

Hypothesis

The researchers hypothesize that Telegram clients may be unsafe for use, as they process the entire set of user data from the original Telegram, including text, image, video, and audio messages, documents, as well as metadata such as geolocation, device information, information about applications on the user’s device, and more. This information may fall into the hands of law enforcement agencies, as well as scammers or other interested parties.

A user who employs a third-party client to restore access to Telegram may face the risk of account hijacking, become a victim of a phishing attack, or be subjected to surveillance by law enforcement agencies. Thoughtlessly downloading an unverified random service can cause many problems.

Methodology

Eight popular alternative Telegram clients for Android were tested. Experts assessed the possible presence of hidden surveillance mechanisms, as well as evidence of data transmission to infrastructure within the reach of Russian security services.

Static Analysis

APK decompilation was performed using jadx (--deobf flag). For each application, the following were analyzed: AndroidManifest.xml (permissions, components, metadata), third-party SDKs (search by packages and domains), network configuration (network_security_config.xml), hardcoded domains and IP addresses.

Dynamic Analysis

Test environment: Android emulator Pixel_7 AVD (API 34, arm64, rooted, writable-system), GPS set to Helsinki (60.1699, 24.9384, EU/GDPR jurisdiction).

Traffic interception: tcpdump on the device (pcap) + mitmproxy 11.1.3 on port 8080 (HTTP proxy with flow recording).

Test scenario (uniform for all applications): launch → attempt login with fake credentials → wait ~90 seconds → uninstall the application to eliminate residual traffic.

SSL unpinning: Frida 17.7.3 with a universal SSL pinning bypass script (Java level). Applied to decrypt Telega traffic.

IP attribution: WHOIS via RIPE NCC (whois.ripe.net). All attributions are based on the org-name and country fields of RIPE records.

Limitations

1. Dynamic analysis covers only the first launch (~90 seconds). Long-term behavior (background services, deferred SDK initialization) was not investigated.

2. SSL certificate pinning at the native level (AppMetrica, VK SDK) blocked decryption of most traffic. Claims about content are based on DNS/SNI (where traffic goes) and static code analysis (what the code sends).
3. Three applications (Graph Messenger, Telega, iMe) required installation via split APK from Google Play due to the App Bundle format.

Analyzed Applications

Application	Version	SHA256
Telegram Official (baseline) `org.telegram.messenger`	`12.4.3`	`795d89d69a0c91ae014482f415582e9ee1590edf1352c754be100ab04a5fd890`
Telegram X `org.thunderdog.challegram`	`0.28.3.1785`	`796cbda361c89033e8f62cba631db27d710e42fde10bb88656962ae3f795c0c3`
Plus Messenger `org.telegram.plus`	`12.4.1.0`	`fa10274fd306a6d4c8ebf65c7f19f6ac8fc43647068975fa4026f45352ed97cf`
Nekogram `tw.nekomimi.nekogram`	`12.4.1`	`ebedfad582a9eb6b932faa5176e817255e6aed50d83fd7d61bb731d75a45d0c0`
Forkgram `org.forkgram.messenger`	`12.4.2.0`	`14fe8a4530893f17f557dedb5c8207c7d929582d495eaa53868eb74e91b0ab62`
Mercurygram `it.belloworld.mercurygram`	`10.14.5.1`	`948403f1589eff2336416218744e16f458588e90e94fbb06181bb5a2902ee8d5`
Graph Messenger `ir.ilmili.telegraph`	`12.3.1.1`	`30a409c3339a23bfecf595e1487e854fc4810befc1ded4dd8a359d523046ab76`
Telega `ru.dahl.messenger`	`2.3.1`	`7558cff2d7929d1e86d5e93296d2a1dcb08ae3e4bcdc7312966a7e0344f649a8`
iMe Messenger `com.iMe.android`	`12.3.3`	`60e6d8c15b552b002271c3ddbd87ce8858482c621abdd2a8571377ad0d953b17`

APKs were obtained from Google Play (Telegram Official, Telegram X, Plus Messenger, Nekogram, Graph Messenger, Telega, iMe) and F-Droid (Forkgram, Mercurygram). Full SHA256 hashes are provided for reproducibility. For applications distributed via App Bundle (split APK), hashes were calculated for the base module.

Research

Stage 1: Static APK Analysis

Decompilation of 9 APKs (8 alternative + baseline) revealed the following patterns.

Analytics and Advertising SDKs

Application	Analytics	Advertising	Firebase Analytics
Telegram Official	0 SDK	0 SDK	Disabled (firebase_analytics_collection_deactivated=true)
Telegram X	0 SDK	0 SDK	Disabled
Plus Messenger	Firebase Analytics	AdMob	Enabled (setAnalyticsCollectionEnabled(true))
Nekogram	Sentry (606 files)	0 SDK	Not disabled (AppMeasurement enabled)
Forkgram	0 SDK	0 SDK	Removed (Firebase completely removed)
Mercurygram	0 SDK	0 SDK	Removed (Firebase completely removed)
Graph Messenger	AppMetrica v7.7.0 (Yandex) + Firebase Analytics	AdMob, AppLovin, Pangle (ByteDance), Facebook, InMobi + proprietary ad system	Enabled
Telega	MyTracker v3.5.0 (VK) + OK.ru AppTracer + Firebase Crashlytics	Proprietary ad system	Disabled (but MyTracker compensates)
iMe	AppMetrica v7.14.0 (Yandex) + Firebase Analytics	AdMob, Yandex Ads, AppLovin, IronSource, Unity, Vungle, InMobi, Pangle (ByteDance), Mail.ru (myTarget), AppNext, Fyber, Mintegral, PubNative, Bigo	Enabled

The official Telegram explicitly disables Firebase Analytics and advertising identifier collection. 3 of 8 alternative clients explicitly enable Firebase Analytics back (Plus Messenger, Graph Messenger, iMe), while 1 more (Nekogram) does not disable it (AppMeasurement enabled). Telega disables Firebase Analytics but compensates with MyTracker (VK Group).

Russian Infrastructure in Code

Application	Russian Domains (not from baseline)	Russian SDKs
Telegram Official	static-maps.yandex.ru (Yandex Maps, server-configurable)	0
Plus Messenger	translate.yandex.net (message translation)	0
Graph Messenger	startup.mobile.yandex.net (AppMetrica)	AppMetrica v7.7.0
Telega	api.telega.info, events.telega.info, stats.dahlmessenger.com, calls.okcdn.ru, api.ok.ru, api.odnoklassniki.ru, sdk-api.apptracer.ru, tracker-api.vk-analytics.ru	MyTracker v3.5.0 (VK), OK.ru SDK, AppTracer
iMe	startup.mobile.yandex.net (AppMetrica), ad.mail.ru (advertising)	AppMetrica v7.14.0, Yandex Ads

Telegram Data Center Substitution (Telega)

The most critical finding of the static analysis is the module ru.dahl.messenger.p014dc in Telega. The application:

1. Requests DC configuration from api.telega.info/v1/dc-proxy
2. Receives a list of alternative IP addresses for all 5 Telegram data centers
3. Replaces the standard Telegram DC addresses (149.154.x.x) with the received ones
4. Can initiate DC configuration reload via push notification (dc_force_switch) — the push carries only a boolean flag; addresses are always fetched from api.telega.info

> The code does not validate that the returned addresses belong to Telegram infrastructure.

User Data Collection (Telega → VK Group)

MyTracker in Telega tracks 30+ event types, including: auth_phone_submit (phone number submission), auth_code_success (successful SMS code verification), auth_cloud_password_success (successful 2FA completion), call_flow_initiated (call initiation).

Each event includes a custom parameter vpn_enabled (added by the Telega developer in Tracker.java, not a standard MyTracker SDK parameter) — VK Group receives deliberately collected information about VPN usage.

The Telegram user ID is explicitly passed to MyTracker via trackLoginEvent(id).

Stage 2: Dynamic Traffic Analysis

Dynamic analysis was conducted for all 9 applications on a unified test environment. Results are presented below in descending order of risk.

Telega

HTTPS requests via proxy (CONNECT):

Destination	Count	Owner
api.telega.info:443	6+3	Telega (Russia)
tracker-api.vk-analytics.ru:443	3+2	VK Group (Russia)
ts.tracker-api.vk-analytics.ru:443	3+2	VK Group (Russia)
ip4.tracker-api.vk-analytics.ru:443	3+2	VK Group (Russia)
firebase-settings.crashlytics.com:443	3	Google
firebaseremoteconfig.googleapis.com:443	6	Google

Direct TCP connections (bypassing HTTP proxy):

IP Address	Port	SYN Packets	Owner (WHOIS)
90.156.232.26	443	17	VK Group, Russia (AS47541)
149.154.167.50	443	8	Telegram, United Kingdom
130.49.152.21	443	2	JSC "TELEGA", Kazan, Russia (AS203502)

Telega is the only application out of 9 that establishes direct TCP connections to IP addresses not belonging to Telegram or Google.

Decrypted Traffic: Data Center Substitution

Using Frida SSL unpinning, the api.telega.info server response was decrypted:

```
GET https://api.telega.info/v1/dc-proxy HTTP/2.0
    user-agent: DAHL-Mobile-App
    x-platform: Android
```

```
HTTP/2.0 200 OK
{
    "dc_version": 2,
    "dcs": [
        {"id": 1, "addresses": [{"host": "130.49.152.50", "port": 443}, ...]},
        {"id": 2, "addresses": [{"host": "130.49.152.21", "port": 443}, ...]},
        {"id": 3, "addresses": [{"host": "130.49.152.52", "port": 443}, ...]},
        {"id": 4, "addresses": [{"host": "130.49.152.53", "port": 443}, ...]},
        {"id": 5, "addresses": [{"host": "130.49.152.14", "port": 443}, ...]}
    ]
}
```

All 25 IP addresses are in the 130.49.152.0/24 subnet, registered to:

```
inetnum:   130.49.152.0 - 130.49.152.255
netname:   JSC-TELEGA
descr:     JOINT STOCK COMPANY "TELEGA" (АО «ТЕЛЕГА»)
address:   ул. Спартаковская 2А / ул. Островского 15и, Казань, Татарстан,
Россия
org:       ORG-JSCT2-RIPE
aut-num:   AS203502
created:   2025-11-05
```

The pcap confirms connection to 130.49.152.21 — the user's MTProto traffic is routed through the JSC "TELEGA" proxy in Kazan.

Substitution scheme:

```
User → [Telega app] → api.telega.info (obtain proxy IPs) → 130.49.152.21 (JSC
"TELEGA", Kazan) → 149.154.x.x (Telegram DC)
```

The operator of the 130.49.152.0/24 servers has the technical capability to: collect metadata (who communicates with whom), log traffic volume and timestamps. As a Russian communications operator, JSC "TELEGA" falls under SORM requirements and the Yarovaya Law, which mandate the storage and provision of data upon request from security services. Whether these capabilities have been exercised in practice was not established by this study.

Graph Messenger

HTTPS requests via proxy:

Destination	Count	Owner
startup.mobile.yandex.net:443	1	Yandex (Russia)
report.appmetrica.yandex.net:443	1	Yandex (Russia)
firebaseremoteconfig.googleapis.com:443	1	Google
firebaseinstallations.googleapis.com:443	1	Google

Direct TCP connections:

IP Address	Port	SYN	Owner (WHOIS)
213.180.204.244	443	1	Yandex LLC, Russia (AS13238)
213.180.193.226	443	1	Yandex LLC, Russia (AS13238)
149.154.167.51	443	1	Telegram, United Kingdom

AppMetrica v7.7.0 actively transmits data to Yandex servers in Russia — both via proxy (CONNECT) and directly (TCP). The SDK runs in a separate process (:AppMetrica) with its own network stack.

iMe

HTTPS requests via proxy:

Destination	Count	Owner
api.imem.app:443	24	iMe (Cloudflare)
firebaseremoteconfig.googleapis.com:443	15	Google
premium.api.imem.app:443	2	iMe
ad.mail.ru:443	1	Mail.ru / VK Group (Russia)

iMe generates 65 CONNECT requests on first launch (baseline: 8). Data transmission to ad.mail.ru (VK Group) confirmed. AppMetrica (Yandex) was not detected during first launch, but is present in the code — deferred initialization is possible.

Plus Messenger

Connection to app-measurement.com confirmed — Firebase Analytics is actively transmitting data. Crashlytics and Remote Config are also active. No direct connections to Russian infrastructure were detected.

A separate static analysis finding: the developer stores user phone numbers and push tokens in Firebase Firestore. The code contains a login code interception mechanism (limited to test numbers, but architecturally can be extended to all users by removing a single condition).

Nekogram

The only non-standard connection is capoo.nekogram.app (developer's server). Sentry SDK (606 files in code) was not detected in traffic during first launch. No connections to Russian infrastructure.

Forkgram

7 CONNECT requests — fewer than the official Telegram (8). The only third-party connection is api.github.com (update checks). Firebase completely removed. Zero analytics, zero advertising.

Mercurygram

3 CONNECT requests (system digitalassetlinks.googleapis.com). Direct TCP connections — only Telegram DC (149.154.167.51, 149.154.175.56). Not a single connection to Google, not a single third-party service. The cleanest network profile among all tested applications.

Telegram X

Telegram X (org.thunderdog.challegram) is an official alternative client from Telegram FZ-LLC, developed by Viacheslav Krylov. Unlike the standard client, it uses TDLib — a cross-platform Telegram library that handles the entire protocol and encryption at the native level. Firebase Analytics is explicitly disabled. No third-party

analytics SDKs. Yandex Maps are absent (unlike the standard client). Permissions are fewer than baseline (34 vs 41), and notably absent are READ_CALL_LOG, WRITE_CONTACTS, CALL_PHONE. Backup is disabled (allowBackup="false") — more secure than baseline.

The network profile is completely identical to the official Telegram: 24 CONNECT requests to Google services, direct TCP only to Telegram DC (149.154.175.50, 149.154.175.56) and Google. Not a single third-party connection.

> Important: Telegram X should not be confused with the trojanized application masquerading under this name (see the "Trojanized Telegram X" section below).

Summary Network Analysis Table

	Application	CONNECT Requests	Russian Domains	Direct TCP to RU	Risks
	Telegram Official (baseline)	8	0	0	-
	Telegram X	24	0	0	Minimal
	Plus Messenger	16	0	0	Medium risk
	Nekogram	16	0	0	Medium risk
	Forkgram	7	0	0	Minimal
	Mercurygram	3	0	0	Minimal
	Graph Messenger	11	2 startup.mobile.yandex.net, report.appmetrica.yandex.net	2 213.180.204.244, 213.180.193.226	High
	Telega	**48+**	**4** api.telega.info, tracker-api.vk-analytics.ru ×3	**2** 90.156.232.26, 130.49.152.21	Critical
	iMe	**65**	**1** ad.mail.ru	0	High

Results

Classification by Risk Level

Telega Critical Risk

Telega is not a Telegram client with cosmetic modifications. It is a fundamentally altered application that:

1. Substitutes Telegram data centers with its own servers belonging to JSC "TELEGA" in Kazan (130.49.152.0/24, AS203502). Confirmed by decrypted HTTPS.
2. Transmits analytics to VK Group via MyTracker (30+ event types, including Telegram user ID, VPN status, authentication flow).
3. Routes calls through OK.ru (calls.okcdn.ru, api.ok.ru) — VK Group infrastructure.
4. Establishes 17 direct TCP connections to VK Group IPs (90.156.232.26) on first launch.

VK Group (formerly Mail.ru Group) is a Russian company with a legal obligation under Federal Law 374 (the “Yarovaya Law”) to provide the FSB with access to user data upon request. The JSC “TELEGA” infrastructure in Kazan is subject to the same laws. This study confirms the technical capability of interception — the actual transfer of data to security services is neither proven nor asserted.

Can Telega Read Messages?

Telega replaces the addresses of all 5 Telegram data centers with its own proxy servers in Kazan (130.49.152.0/24). All MTProto traffic passes through these servers. The proxy operator is guaranteed to see metadata: who communicates with whom, when, how often, and how much data is transferred.

The content of regular chats is protected by MTProto encryption between the client and Telegram servers. However, the proxy operator is in a man-in-the-middle position: if the proxy does not simply relay the TCP stream but terminates the TLS connection, access to the content is technically possible. Whether the operator actually reads message content was not

established during this study — doing so would require analysis of the protocol on the proxy server side.

In parallel, MyTracker (VK Group) receives the user's Telegram user ID, VPN status, and detailed event flow (authentication, calls, invitations) — this is metadata available to VK Group unconditionally.

Graph Messenger High Risk

1. Yandex AppMetrica v7.7.0 actively transmits data to YANDEX LLC servers in Russia. Confirmed by CONNECT requests to startup.mobile.yandex.net, report.appmetrica.yandex.net and direct TCP to 213.180.193.226, 213.180.204.244.
2. 6 advertising SDKs, including Pangle (ByteDance/TikTok, China).
3. Proprietary advertising system with a database that includes fields for APK distribution (apk_url, apk_pkg).
4. Firebase Analytics enabled (the official Telegram disables it).
5. Device fingerprinting based on IMEI/MAC address with a unique "ilmili" identifier.

iMe Messenger High Risk

1. 15+ advertising SDKs — the highest number among all tested apps. Includes Yandex Ads, Mail.ru (myTarget), Pangle (ByteDance).
2. AppMetrica v7.14.0 found in the code (static analysis; not detected in traffic during first launch — deferred initialization possible).
3. ad.mail.ru (confirmed dynamically) — data transmitted to VK Group.
4. 65 CONNECT requests on first launch (baseline: 8), of which 24 go to the developer's own backend api.imem.app.
5. Crypto wallet with operations through the developer's backend — iMe can see user addresses and transactions.

Plus Messenger Medium risk

1. Firebase Analytics enabled (confirmed: app-measurement.com). 14 additional permissions vs baseline.
2. Firebase Firestore stores phone numbers and push tokens on the developer's server.
3. Login code interception mechanism (limited to test numbers).
4. Dangerous permissions: SEND_SMS, READ_LOGS, MANAGE_EXTERNAL_STORAGE.
5. Yandex Translation API sends message text to translate.yandex.net when using the translation feature.

Nekogram Medium risk

1. Sentry SDK (606 files) — crash reporting with session replay capability. Not detected in traffic.
2. Firebase Analytics not disabled (AppMeasurement services enabled).
3. Developer's own server capoo.nekogram.app (purpose unknown).
4. String obfuscation hinders auditing.
5. Chinese translation services (Baidu, Tencent, Sogou, Youdao) — when used, message text is processed within PRC jurisdiction.

Forkgram Minimal Risk

1. De-Googled: Firebase, Google Play Services, Google Maps completely removed.
2. Less traffic than baseline (7 CONNECT vs 8).
3. Updates via GitHub (open platform).
4. No analytics, no advertising, no developer servers.

Mercurygram Minimal Risk

1. Absolute minimum: 3 CONNECT requests (system only), 0 third-party services.
2. Only Telegram DC in direct TCP connections.
3. FOSS-oriented fork based on Telegram-FOSS.
4. No Firebase, no Google, no analytics.

Key Findings

1. Telegram Data Center Substitution. Telega replaces 5 standard Telegram DCs with 25 IP addresses in Kazan (JSC "TELEGA"). All MTProto traffic passes through Russian proxies. This is not a theoretical vulnerability — the substitution has been confirmed by decrypted HTTPS.

2. 3 of 8 alternative clients transmit data to Russia — Telega (VK Group + JSC "TELEGA"), Graph Messenger (Yandex), iMe (Mail.ru/VK Group). For Telega this is the primary data transmission channel; for Graph Messenger and iMe it is a side effect (via analytics and advertising SDKs).

3. 3 of 8 clients explicitly enable Firebase Analytics (Plus Messenger, Graph Messenger, iMe), while 1 more (Nekogram) does not disable it. The official Telegram explicitly deactivates Firebase Analytics — alternative clients reverse this decision, and Google receives data about messenger usage.

4. Mercurygram and Forkgram are the only forks that generate less network traffic than the official Telegram. Both have completely removed Firebase and Google services.

5. The number of advertising SDKs correlates with risk: Graph Messenger (6 SDKs), iMe (15+ SDKs), Plus Messenger (1 SDK) — all contain potentially dangerous data collection mechanisms.

6. VK Group is present in two applications: Telega (MyTracker, OK.ru) and iMe (ad.mail.ru). VK Group is Russia’s largest internet holding company with a legal obligation to provide data to security services upon request (Federal Law 374).

Additional Finding: Trojanized "Telegram X"

During the study, an application was discovered being distributed under the name "Telegram X" (package plenty.oceanbyte.web, SHA256: 7e65c8015d722e6b736472e0a33e94bae09fdf28328de700ca47ff9ebf898389). The distribution channel has not been established — the manifest contains a reference to Play Store ID only.u.android, but the app’s presence on Google Play has not been confirmed. This is not an alternative client but a fully functional trojan with C2 infrastructure codenamed "WorldPeace" (v3.0.5).

The application contains:

1. Telegram session theft — upon account login, exports the tgnet.dat file (MTProto session keys) to the C2 server hpncallback.qxgolds.com. Enables full account takeover.
2. Message interception and substitution — monitoring of incoming/outgoing messages by regular expressions with the ability to replace content.
3. Clipboard exfiltration — on every app resume (target vector: crypto wallets, passwords).
4. Redis C2 channel — persistent pub/sub connection to 159.138.237.10:33619 for remote control (forced channel joins, command reception).
5. Heartbeat approximately every 3 minutes — transmitting phone number, username, password, IP address, IMEI/MEID, Advertising ID.
6. Collection of IMEI, MEID, serial number, device fingerprint.

Debug strings in the code are in Simplified Chinese; country targeting: Southeast Asia (Philippines, Thailand, Myanmar, Cambodia, Laos), Africa (South Africa, Angola), Indonesia, Hong Kong.

IoC: domain hpncallback.qxgolds.com, IP 159.138.237.10 (Huawei Cloud Thailand, AS136907), port 33619. The full set of indicators of compromise, including credentials, has been submitted to relevant CERT organizations.

> This trojan is not associated with the alternative clients under study and represents a different threat category — not metadata collection via SDKs, but targeted spyware. It is included in this report as an illustration of the risks of installing Telegram clients from unverified sources.

Recommendations for Users

1. Use the official Telegram client. This is the only client whose code is maintained by the Telegram team and undergoes regular community auditing. Any third-party client — even one that is clean at the time of review — can change its behavior in the next update without the user's knowledge.
2. Do not use Telega (ru.dahl.messenger) — the DC substitution makes the messenger unsuitable for confidential communication.
3. Do not use Graph Messenger or iMe for sensitive communications due to data transmission to Yandex and VK Group servers.
4. Mercurygram and Forkgram showed a clean network profile at the time of the study with no data transmission to third parties. However, this is no guarantee for the future — developers can add any data collection mechanisms in the next version.
5. When using Plus Messenger, be aware that Firebase Analytics is active and the developer stores data on their Firebase backend.
6. When using Nekogram, avoid Chinese translation services (Baidu, Tencent, Sogou, Youdao).

Questions for Further Research

1. How exactly does JSC "TELEGA" handle proxied MTProto traffic? Is only relay performed, or is logging also conducted?
2. What is the corporate relationship between JSC "TELEGA" and VK Group? The use of OK.ru SDK and MyTracker indicates a close partnership.
3. Is Telegram aware of the DC substitution in Telega, and does it plan to take action?
4. How might the use of Yandex Maps add risks when used with the official Telegram client?