RKS Global

rks.global

Тестирование альтернативных Telegram-клиентов

Анализ 8 альтернативных Telegram-клиентов для Android на факт передачи данных на российскую инфраструктуру и наличие скрытых механизмов слежки

Содержание

Гипотеза

Гипотеза исследователей состоит в том, что клиенты Telegram могут быть небезопасны для использования, так как они обрабатывают весь массив данных пользователей оригинального Telegram, включая текстовые, графические, видео- и аудио-сообщения, документы, а также метаданные, в частности, геолокацию, информацию об устройстве пользователя, приложениях на его устройстве и пр. Эта информация может попасть в руки представителей силовых структур, а также мошенников или других заинтересованных лиц.

Пользователь, который использует сторонний клиент для восстановления доступа к Telegram, может столкнуться с риском угона аккаунта, стать жертвой фишинговой атаки или преследования со стороны правоохранительных органов. Необдуманно скачанный непроверенный случайный сервис может принести много проблем.

Методология

Протестировано восемь популярных альтернативных Telegram-клиентов для Android. Эксперты устанавливали возможности наличия скрытых механизмов слежки, а также факт передачи ими данных на инфраструктуру, находящуюся в пределах досягаемости российских силовиков.

Статический анализ

Декомпиляция APK выполнена с помощью jadx (флаг --deobf). Для каждого приложения проанализированы: AndroidManifest.xml (разрешения, компоненты, метаданные), третьесторонние SDK (поиск по пакетам и доменам), сетевая конфигурация (network_security_config.xml), захардкоженные домены и IP-адреса.

Динамический анализ

Стенд: Android-эмулятор Pixel_7 AVD (API 34, arm64, rooted, writable-system), GPS - Хельсинки (60.1699, 24.9384, юрисдикция EC/GDPR).

Перехват трафика: tcpdump на устройстве (pcap) + mitmproxy 11.1.3 на порту 8080 (HTTP-прокси с записью flow).

Тестовый сценарий (единый для всех приложений): запуск → попытка входа с фейковыми данными → ожидание ~90 секунд → удаление приложения для исключения паразитного трафика.

SSL unpinning: Frida 17.7.3 с универсальным скриптом обхода SSL-пиннинга (Java-уровень). Применён для расшифровки трафика Telega.

Атрибуция IP: WHOIS через RIPE NCC (whois.ripe.net). Все атрибуции основаны на полях org-name и country записей RIPE.

Ограничения

1. Динамический анализ охватывает только первый запуск (~90 секунд). Долгосрочное поведение (фоновые сервисы, отложенная инициализация SDK) не исследовалось.
2. SSL certificate pinning на нативном уровне (AppMetrica, VK SDK) заблокировал расшифровку большей части трафика. Утверждения о содержимом основаны на DNS/SNI (куда идёт трафик) и статическом анализе кода (что код отправляет).
3. Три приложения (Graph Messenger, Telega, iMe) потребовали установки через split APK с Google Play из-за App Bundle формата.

Проанализированные приложения

Приложение и пакет	Версия	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`

Приложение и пакет	Версия	SHA256
Telega `ru.dahl.messenger`	`2.3.1`	`7558cff2d7929d1e86d5e93296d2a1dcb08ae3e4bcdc7312966a7e0344f649a8`
iMe Messenger `com.iMe.android`	`12.3.3`	`60e6d8c15b552b002271c3ddbd87ce8858482c621abdd2a8571377ad0d953b17`

APK получены из Google Play (Telegram Official, Telegram X, Plus Messenger, Nekogram, Graph Messenger, Telega, iMe) и F-Droid (Forkgram, Mercurygram). Полные SHA256-хеши приведены для воспроизводимости. Для приложений, распространяемых через App Bundle (split APK), хеши рассчитаны для базового модуля.

Исследование

Этап 1: Статический анализ APK

Декомпиляция 9 APK (8 альтернативных + baseline) выявила следующие паттерны.

Аналитические и рекламные SDK

Приложение	Аналитика	Реклама	Firebase Analytics
Telegram Official	0 SDK	0 SDK	Отключён (firebase_analytics_collection_deactivated=true)
Telegram X	0 SDK	0 SDK	Отключён
Plus Messenger	Firebase Analytics	AdMob	Включён (setAnalyticsCollectionEnabled(true))
Nekogram	Sentry (606 файлов)	0 SDK	Не отключён (AppMeasurement enabled)
Forkgram	0 SDK	0 SDK	Удалён (Firebase полностью удалён)
Mercurygram	0 SDK	0 SDK	Удалён (Firebase полностью удалён)
Graph Messenger	AppMetrica v7.7.0 (Яндекс) + Firebase Analytics	AdMob, AppLovin, Pangle (ByteDance), Facebook, InMobi + собственная рекламная система	Включён
Telega	MyTracker v3.5.0 (VK) + OK.ru AppTracer + Firebase Crashlytics	Собственная рекламная система	Отключён (но MyTracker компенсирует)
iMe	AppMetrica v7.14.0 (Яндекс) + Firebase Analytics	AdMob, Yandex Ads, AppLovin, IronSource, Unity, Vungle, InMobi, Pangle (ByteDance), Mail.ru (myTarget), AppNext, Fyber, Mintegral, PubNative, Bigo	Включён

Официальный Telegram явно отключает Firebase Analytics и сбор рекламного идентификатора. 3 из 8 альтернативных клиентов явно включают Firebase Analytics обратно (Plus Messenger, Graph Messenger, iMe), ещё 1 (Nekogram) не отключает его (AppMeasurement enabled). Telega отключает Firebase Analytics, но компенсирует это MyTracker (VK Group).

Российская инфраструктура в коде

Приложение	Российские домены (не из baseline)	Российские SDK
Telegram Official	static-maps.yandex.ru (Яндекс.Карты, server-configurable)	0
Plus Messenger	translate.yandex.net (перевод сообщений)	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 (реклама)	AppMetrica v7.14.0, Yandex Ads

Подмена дата-центров Telegram (Telega)

Самая критичная находка статического анализа - модуль ru.dahl.messenger.p014dc в Telega. Приложение:

1. Запрашивает конфигурацию DC с api.telega.info/v1/dc-proxy
2. Получает список альтернативных IP-адресов для всех 5 дата-центров Telegram
3. Подменяет стандартные адреса Telegram DC (149.154.x.x) на полученные

4. Может инициировать повторную загрузку конфигурации DC по push-уведомлению (dc_force_switch) - push несёт только булевый флаг, адреса всегда загружаются с api.telega.info

> Код не валидирует, что возвращённые адреса принадлежат инфраструктуре Telegram.

Сбор данных пользователя (Telega → VK Group)

MyTracker в Telega отслеживает 30+ типов событий, включая: - auth_phone_submit - отправка номера телефона - auth_code_success - успешная верификация SMS-кода - auth_cloud_password_success - успешное прохождение 2FA - call_flow_initiated - начало звонка

Каждое событие включает кастомный параметр vpn_enabled (добавлен разработчиком Telega в Tracker.java, не является стандартным параметром MyTracker SDK) - VK Group получает целенаправленно собранную информацию об использовании VPN.

Telegram user ID явно передаётся в MyTracker через trackLoginEvent(id).

Этап 2: Динамический анализ трафика

Динамический анализ проведён для всех 9 приложений на едином стенде. Результаты представлены ниже в порядке убывания риска.

Telega

HTTPS-запросы через прокси (CONNECT):

Назначение	Количество	Владелец
api.telega.info:443	6+3	Телега (Россия)
tracker-api.vk-analytics.ru:443	3+2	VK Group (Россия)
ts.tracker-api.vk-analytics.ru:443	3+2	VK Group (Россия)
ip4.tracker-api.vk-analytics.ru:443	3+2	VK Group (Россия)
firebase-settings.crashlytics.com:443	3	Google
firebaseremoteconfig.googleapis.com:443	6	Google

Прямые TCP-соединения (минуя HTTP-прокси):

IP-адрес	Порт	SYN-пакетов	Владелец (WHOIS)
90.156.232.26	443	17	VK Group, Россия (AS47541)
149.154.167.50	443	8	Telegram, Великобритания
130.49.152.21	443	2	АО «ТЕЛЕГА», Казань, Россия (AS203502)

Telega - единственное приложение из 9, устанавливающее прямые TCP-соединения с IP-адресами, не принадлежащими Telegram или Google.

Расшифрованный трафик: подмена дата-центров

При помощи Frida SSL unpinning расшифрован ответ сервера api.telega.info:

```
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}, ...]}
    ]
}
```

Все 25 IP-адресов находятся в подсети 130.49.152.0/24, зарегистрированной на:

```
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
```

Pcap подтверждает подключение к 130.49.152.21 - MTProto-трафик пользователя маршрутизируется через прокси АО «ТЕЛЕГА» в Казани.

Схема подмены:

```
Пользователь → [Telega app] → api.telega.info (получить IP прокси)→
130.49.152.21 (АО «ТЕЛЕГА», Казань) → 149.154.x.x (Telegram DC)
```

Оператор серверов 130.49.152.0/24 имеет техническую возможность: собирать метаданные (кто с кем общается), логировать объём трафика и таймстампы. Как российский оператор связи, АО «ТЕЛЕГА» подпадает под требования СОРМ и закона Яровой, обязывающие хранить и предоставлять данные по запросу спецслужб. Факт реализации этих возможностей на практике настоящим исследованием не установлен.

Graph Messenger

HTTPS-запросы через прокси:

Назначение	Кол-во	Владелец
startup.mobile.yandex.net:443	1	Yandex (Россия)
report.appmetrica.yandex.net:443	1	Yandex (Россия)
firebaseremoteconfig.googleapis.com:443	1	Google
firebaseinstallations.googleapis.com:443	1	Google

Прямые TCP-соединения:

IP-адрес	Порт	SYN	Владелец (WHOIS)
213.180.204.244	443	1	Yandex LLC, Россия (AS13238)
213.180.193.226	443	1	Yandex LLC, Россия (AS13238)
149.154.167.51	443	1	Telegram, Великобритания

AppMetrica v7.7.0 активно передаёт данные на серверы Яндекса в России - как через прокси (CONNECT), так и напрямую (TCP). SDK работает в отдельном процессе (:AppMetrica) с собственным сетевым стеком.

iMe

HTTPS-запросы через прокси:

Назначение	Кол-во	Владелец
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 (Россия)

iMe генерирует 65 CONNECT-запросов при первом запуске (baseline - 8). Подтверждена передача данных на ad.mail.ru (VK Group). AppMetrica (Yandex) не

зафиксирована при первом запуске, но присутствует в коде - возможна отложенная инициализация.

Plus Messenger

Подтверждено соединение с app-measurement.com - Firebase Analytics активно передаёт данные. Также активны Crashlytics и Remote Config. Прямых подключений к российской инфраструктуре не обнаружено.

Отдельная находка статического анализа: разработчик хранит номера телефонов пользователей и push-токены в Firebase Firestore. Код содержит механизм перехвата кодов входа (ограничен тестовыми номерами, но архитектурно может быть расширен на всех пользователей удалением одного условия).

Nekogram

Единственное нестандартное подключение - capoo.nekogram.app (сервер разработчика). Sentry SDK (606 файлов в коде) не зафиксирован в трафике при первом запуске. Подключений к российской инфраструктуре нет.

Forkgram

7 CONNECT-запросов – меньше, чем у официального Telegram (8). Единственное стороннее подключение - api.github.com (проверка обновлений). Firebase полностью удалён. Ноль аналитики, ноль рекламы.

Mercurygram

3 CONNECT-запроса (системный digitalassetlinks.googleapis.com). Прямые TCP - только Telegram DC (149.154.167.51, 149.154.175.56). Ни одного соединения с Google, ни одного стороннего сервиса. Самый чистый сетевой профиль среди всех протестированных приложений.

Telegram X

Telegram X (org.thunderdog.challegram) - официальный альтернативный клиент от Telegram FZ-LLC, разработанный Viacheslav Krylov. В отличие от стандартного клиента, использует TDLib - кроссплатформенную библиотеку Telegram, обрабатывающую весь протокол и шифрование на нативном уровне. Firebase Analytics явно отключён. Третьесторонних аналитических SDK нет. Яндекс.Карты отсутствуют (в отличие от стандартного клиента). Разрешений меньше, чем у baseline (34 vs 41), при этом отсутствуют READ_CALL_LOG, WRITE_CONTACTS, CALL_PHONE. Резервное копирование отключено (allowBackup="false") - безопаснее baseline.

Сетевой профиль полностью аналогичен официальному Telegram: 24 CONNECT-запроса к Google-сервисам, прямые TCP - только к Telegram DC (149.154.175.50, 149.154.175.56) и Google. Ни одного стороннего подключения.

> Важно: Telegram X не следует путать с троянизированным приложением, маскирующимся под это название (см. раздел «Троянизированный Telegram X» ниже).

Сводная таблица сетевого анализа

	Приложение	CONNECT-запросов	Российские домены	Прямые TCP к РФ	Риски
	Telegram Official (baseline)	8	0	0	-
	Telegram X	24	0	0	Минимальный
	Plus Messenger	16	0	0	Средний риск
	Nekogram	16	0	0	Средний риск
	Forkgram	7	0	0	Минимальный
	Mercurygram	3	0	0	Минимальный
	Graph Messenger	11	**2** `startup.mobile.yandex.net`, `report.appmetrica.yandex.net`	**2** `213.180.204.244`, `213.180.193.226`	Высокий
	Telega	**48+**	**4** `api.telega.info`, `tracker-api.vk-analytics.ru` ×3	**2** `90.156.232.26`, `130.49.152.21`	Критический
	iMe	**65**	**1** `ad.mail.ru`	0	Высокий

Результаты

Классификация по уровню риска

 **Критический риск**

Telega — не Telegram-клиент с косметическими модификациями. Это фундаментально изменённое приложение, которое:

1. Подменяет дата-центры Telegram на собственные серверы АО «ТЕЛЕГА» в Казани (130.49.152.0/24, AS203502). Подтверждено расшифрованным HTTPS.
2. Передаёт аналитику VK Group через MyTracker (30+ типов событий, включая Telegram user ID, статус VPN, поток аутентификации).
3. Маршрутизирует звонки через OK.ru (calls.okcdn.ru, api.ok.ru) - инфраструктуру VK Group.
4. Устанавливает 17 прямых TCP-соединений с IP VK Group (90.156.232.26) при первом запуске.

VK Group (ранее Mail.ru Group) – российская компания, имеющая законодательную обязанность по ФЗ-374 («закон Яровой») предоставлять ФСБ доступ к данным пользователей по запросу. Инфраструктура АО «ТЕЛЕГА» в Казани подпадает под те же законы. Настоящее исследование подтверждает техническую возможность перехвата - факт передачи данных спецслужбам не доказан и не утверждается.

Может ли Telega читать сообщения?

Telega подменяет адреса всех 5 дата-центров Telegram на собственные прокси-серверы в Казани (130.49.152.0/24). Весь MTProto-трафик проходит через эти серверы. Оператор прокси гарантированно видит метаданные: кто с кем общается, когда, как часто, какой объём данных передаётся.

Содержимое обычных чатов защищено шифрованием MTProto между клиентом и серверами Telegram. Однако оператор прокси находится в позиции man-in-the-middle: если прокси не просто ретранслирует TCP-поток, а терминирует TLS-соединение, доступ

к содержимому технически возможен. Факт чтения содержимого сообщений оператором в ходе данного исследования не установлен – для этого потребовался бы анализ протокола на стороне прокси-сервера.

Параллельно MyTracker (VK Group) получает Telegram user ID пользователя, статус VPN и детальный поток событий (аутентификация, звонки, приглашения) – это метаданные, доступные VK Group безусловно.

Graph Messenger Высокий риск

1. Yandex AppMetrica v7.7.0 активно передаёт данные на серверы YANDEX LLC в России. Подтверждено CONNECT-запросами к startup.mobile.yandex.net, report.appmetrica.yandex.net и прямыми TCP к 213.180.193.226, 213.180.204.244.
2. 6 рекламных SDK, включая Pangle (ByteDance/TikTok, Китай).
3. Собственная рекламная система с базой данных, включающей поля для распространения APK (apk_url, apk_pkg).
4. Firebase Analytics включён (официальный Telegram его отключает).
5. Device fingerprinting на основе IMEI/MAC-адреса с уникальным идентификатором "ilmili".

iMe Messenger Высокий риск

1. 15+ рекламных SDK – максимальное количество среди всех протестированных. Включает Yandex Ads, Mail.ru (myTarget), Pangle (ByteDance).
2. AppMetrica v7.14.0 обнаружена в коде (статический анализ; не зафиксирована в трафике при первом запуске – возможна отложенная инициализация).
3. ad.mail.ru (подтверждено динамически) – данные передаются на VK Group.
4. 65 CONNECT-запросов при первом запуске (baseline – 8), из них 24 к собственному бэкенду api.imem.app.
5. Крипто-кошелёк с операциями через бэкенд разработчика - iMe может видеть адреса и транзакции пользователей.

Plus Messenger Средний риск

1. Firebase Analytics включён (подтверждено: app-measurement.com). 14 дополнительных разрешений vs baseline.
2. Firebase Firestore хранит номера телефонов и push-токены на сервере разработчика.
3. Механизм перехвата кодов входа (ограничен тестовыми номерами).
4. Опасные разрешения: SEND_SMS, READ_LOGS, MANAGE_EXTERNAL_STORAGE.
5. Yandex Translation API отправляет текст сообщений на translate.yandex.net при использовании функции перевода.

Nekogram Средний риск

1. Sentry SDK (606 файлов) – crash reporting с возможностью session replay.
   Не зафиксирован в трафике.
2. Firebase Analytics не отключён (AppMeasurement services enabled).
3. Собственный сервер capoo.nekogram.app (назначение неизвестно).
4. Обфускация строк затрудняет аудит.
5. Китайские сервисы перевода (Baidu, Tencent, Sogou, Youdao) – при использовании текст сообщений обрабатывается в юрисдикции КНР.

Forkgram Минимальный риск

1. De-Googled: Firebase, Google Play Services, Google Maps полностью удалены.
2. Меньше трафика, чем baseline (7 CONNECT vs 8).
3. Обновления через GitHub (открытая платформа).
4. Нет аналитики, нет рекламы, нет серверов разработчика.

Mercurygram **Минимальный риск**

1. Абсолютный минимум: 3 CONNECT-запроса (только системные), 0 сторонних сервисов.
2. Только Telegram DC в прямых TCP-соединениях.
3. FOSS-ориентированный форк на базе Telegram-FOSS.
4. Нет Firebase, нет Google, нет аналитики.

Ключевые выводы

1. Подмена дата-центров Telegram. Telega заменяет 5 стандартных DC Telegram на 25 IP-адресов в Казани (АО «ТЕЛЕГА»). Весь MTProto-трафик проходит через российские прокси. Это не теоретическая уязвимость – подмена подтверждена расшифрованным HTTPS.

2. 3 из 8 альтернативных клиентов передают данные в Россию – Telega (VK Group + АО «ТЕЛЕГА»), Graph Messenger (Yandex), iMe (Mail.ru/VK Group). Для Telega это основной канал передачи; для Graph Messenger и iMe – побочный (через аналитические и рекламные SDK).

3. 3 из 8 клиентов явно включают Firebase Analytics (Plus Messenger, Graph Messenger, iMe), ещё 1 (Nekogram) не отключает его. Официальный Telegram явно деактивирует Firebase Analytics – альтернативные клиенты отменяют это решение, и Google получает данные об использовании мессенджера.

4. Mercurygram и Forkgram – единственные форки, генерирующие меньше сетевого трафика, чем официальный Telegram. Оба полностью удалили Firebase и Google-сервисы.

5. Количество рекламных SDK коррелирует с риском: Graph Messenger (6 SDK), iMe (15+ SDK), Plus Messenger (1 SDK) – все содержат потенциально опасные механизмы сбора данных.

6. VK Group присутствует в двух приложениях: Telega (MyTracker, OK.ru) и iMe (ad.mail.ru). VK Group – крупнейший российский интернет-холдинг, имеющий законодательную обязанность предоставлять данные по запросу спецслужб (ФЗ-374).

Дополнительная находка: троянизированный «Telegram X»

В ходе исследования обнаружено приложение, распространяющееся под названием «Telegram X» (пакет plenty.oceanbyte.web, SHA256: 7e65c8015d722e6b736472e0a33e94bae09fdf28328de700ca47ff9ebf898389). Канал распространения не установлен - манифест содержит ссылку на Play Store ID only.u.android, но наличие приложения в Google Play не подтверждено. Это не альтернативный клиент, а полноценный троян с C2-инфраструктурой под кодовым названием «WorldPeace» (v3.0.5).

Приложение содержит:

1. Кражу сессии Telegram - при входе в аккаунт экспортирует файл tgnet.dat (MTProto-ключи сессии) на C2-сервер hpncallback.qxgolds.com. Позволяет полный захват аккаунта.
2. Перехват и подмену сообщений – мониторинг входящих/исходящих сообщений по регулярным выражениям с возможностью замены содержимого.
3. Эксфильтрацию буфера обмена - при каждом возобновлении приложения (целевой вектор - криптокошельки, пароли).
4. Redis C2-канал – постоянное pub/sub-соединение с 159.138.237.10:33619 для удалённого управления (принудительное вступление в каналы, получение команд).
5. Heartbeat каждые ~3 минуты – передача номера телефона, username, пароля, IP-адреса, IMEI/MEID, Advertising ID.
6. Сбор IMEI, MEID, серийного номера, отпечатка устройства.

Отладочные строки в коде на упрощённом китайском, таргетинг по странам: ЮВА (Филиппины, Таиланд, Мьянма, Камбоджа, Лаос), Африка (ЮАР, Ангола), Индонезия, Гонконг.

IoC: домен hpncallback.qxgolds.com, IP 159.138.237.10 (Huawei Cloud Thailand, AS136907), порт 33619. Полный набор индикаторов компрометации, включая credentials, передан в профильные CERT-организации.

> Данный троян не связан с исследуемыми альтернативными клиентами и представляет иную категорию угрозы - не сбор метаданных через SDK, а целенаправленное шпионское ПО. Включён в отчёт как иллюстрация рисков установки Telegram-клиентов из непроверенных источников.

Рекомендации для пользователей

1. Использовать официальный клиент Telegram. Это единственный клиент, код которого поддерживается командой Telegram и проходит регулярный аудит сообществом. Любой сторонний клиент – даже чистый на момент проверки – может изменить поведение в следующем обновлении без ведома пользователя.
2. Не использовать Telega (ru.dahl.messenger) – подмена DC делает мессенджер непригодным для конфиденциальной переписки.
3. Не использовать Graph Messenger и iMe для чувствительных коммуникаций из-за передачи данных на серверы Яндекса и VK Group.
4. Mercurygram и Forkgram на момент исследования показали чистый сетевой профиль без передачи данных третьим сторонам. Однако это не гарантия на будущее - разработчики могут добавить любые механизмы сбора данных в следующей версии.
5. При использовании Plus Messenger следует учитывать, что Firebase Analytics активен и разработчик хранит данные на своём Firebase-бэкенде.
6. При использовании Nekogram – избегать китайских сервисов перевода (Baidu, Tencent, Sogou, Youdao).

Вопросы для дальнейшего исследования

1. Как именно АО «ТЕЛЕГА» обрабатывает проксируемый MTProto-трафик? Выполняется ли только ретрансляция или также логирование?
2. Какова корпоративная связь АО «ТЕЛЕГА» с VK Group? Использование OK.ru SDK и MyTracker указывает на тесное партнёрство.
3. Осведомлён ли Telegram о подмене DC в Telega и планирует ли предпринять меры?
4. Как использование Яндекс Карт может добавлять риски при использовании официальным клиентом Telegram?