НОВИНИ

Оперативна інформація щодо російського вторгнення станом на 16:00 24.05.2026
24 ТРА, 2026

Затримано мародера, який після ракетного обстрілу обкрадав пошкоджені квартири на столичному Подолі
24 ТРА, 2026

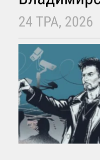
У ДТП на Львівщині загинув водій вантажівки (фото)
24 ТРА, 2026

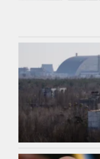
Понад ₴800 тис. збитків – митника судитимуть за махінації з експортом олії
24 ТРА, 2026

У Вашингтоні біля Білого дому застрелили чоловіка, який відкрив вогонь
24 ТРА, 2026

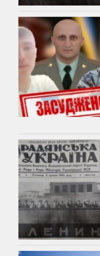
Військовозобов'язаний застрелився у приміщенні Тернопільського обласного ТЦК
24 ТРА, 2026

Сили Оборони України атакували нафтоперекачувальну станцію «Второво» у Владимирській області РФ
24 ТРА, 2026


Незалежна експертиза підтвердила критичну вразливість «Телеграму». Під загрозою приватність мільйонів користувачів
24 ТРА, 2026

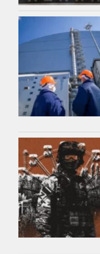

Чорнобильська ЧАЕС на паузі: 40 років без рішень і нові загрози
25 КВІ, 2026

Українські суди оголосили нові вироки за воєнні злочини російських загарбників, але є проблеми
25 КВІ, 2026



14 секунд правди: як Чорнобильська катастрофа підірвала радянську імперію
26 КВІ, 2026

Привид Фукусіми на берегах Прип'яті: чому блекаути в Чорнобилі стали критичною загрозою
26 КВІ, 2026


Ядерний тероризм Росії як тактика: чому МАГАТЕ виявилося безсилим перед окупацією ЗАЕС та ЧАЕС
26 КВІ, 2026

Кінець морських авантюр: як українські дрони поховали десантні надії Кремля у Севастополі
27 КВІ, 2026

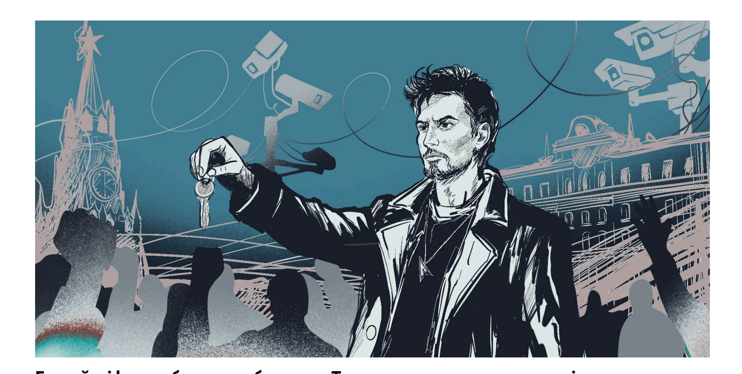
COVID-19 ДТП Донбасс Київ Розшук дітей агрессия России атака дронами-камікадзе вбивство вбивство мирних жителів вимагання війна війна с Россией воєнні злочини РФ втрати окупантів війна з Росією грабіж державна зрада допомога союзників Україні замах на вбивство зловживання службовим становищем знищення окупантів колабораційна діяльність коронавирус коррупция корупція крадіжка напад Росії на Україну наркозлочини незаконне переправлення осіб через держкордон ножове поранення обстріли цивільної інфраструктури оперативна інформація пособники окупантів привласнення коштів підроблення документів п'яний за кермом ракетні удари окупантів розбій російські воєнні злочинці русский мир смертельна ДТП убийство хабар хуліганство шахрайство

РЕКЛАМА

ГОЛОВНЕ / РОЗСЛІДУВАННЯ

Незалежна експертиза підтвердила критичну вразливість «Телеграму». Під загрозою приватність мільйонів користувачів

PUBLISHED 24 ТРАВНЯ 2026



Гучний міф про абсолютну безпеку «Телеграму» остаточно розлетівся на друзки після того, як колишній фінансовий директор месенджера Володимир Веденєєв невдало сходив до швейцарського суду. Намагаючись спростувати розслідування журналістів, топменеджер сам додав до матеріалів справи експертний звіт компанії Symbolic Software, яка замість виправдання підтвердила катастрофічну вразливість.

З'ясувалося, що додаток Павла Дурова свідомо ігнорує базове транспортне шифрування, передаючи унікальні ідентифікатори пристроїв у відкритому вигляді. У поєднанні із зізнаннями самого Веденєєва про наявність у нього прямого куратора з ФСБ та оперативного надання адрес і прізвищ користувачів за першим же кліком, «головний інструмент європейських активістів» офіційно перетворився на слухняну цифрову магістраль під контролем Луб'янки.

У розпорядженні журналістів «Важливих історій» опинився експертний звіт компанії Symbolic Software, яка спеціалізується на аналізі кібербезпеки та технічному аудиті додатків для таких IT-гігантів, як Zoom, Mozilla, Coinbase та багатьох інших. Symbolic Software перевірила твердження з минулорічної публікації «Важливих історій» про те, як «Телеграм» пов'язаний з ФСБ, і дійшла висновку, що описана нами у 2025 році вразливість дійсно загрожує приватності всіх користувачів месенджера, включаючи навіть тих, хто листується в секретних чатах.

«Ми перевірили твердження з публікації щодо цих вразливостей і дійшли висновку, що основні технічні висновки є правильними і їх можна підтвердити незалежним способом. <…> Наслідки цієї уразливості виходять далеко за межі теоретичних побоювань. <…> Це особливо важливо, враховуючи, що «Телеграм» широко використовується журналістами, активістами та іншими людьми з груп підвищеного ризику», — йдеться в експертизі (повний звіт Symbolic Software можна прочитати тут).

> *Терор у Telegram: 85% диверсантів — це не агенти ФСБ, а звичайні люди у скруті, яких рашисти "програмують" на вбивство*

Про яку вразливість йдеться?

Під час роботи над минулорічним розслідуванням «Важливі історії» провели експеримент: попросили людей у різних країнах світу надіслати одне одному повідомлення в «Телеграмі» та записати трафік за допомогою спеціальної програми. Потім ми показали отримані результати експертам у галузі кібербезпеки, і вони виявили, що під час передачі даних месенджер надсилає незашифрований заголовок, що містить унікальний ідентифікатор пристрою auth_key_id.

За допомогою цього ідентифікатора ті, хто має доступ до трафіку «Телеграму», можуть стежити за користувачами, аналізувати їхню мережеву активність та виявляти комунікаційні зв'язки. Експерти з Symbolic Software дійшли такого самого висновку: «Наш аналіз підтверджує ключові технічні висновки: «Телеграм» передає повідомлення через незахищені TCP-з'єднання, через що ідентифікатор auth_key_id надсилається у відкритому вигляді або у формі, яку легко розшифрувати будь-якому посереднику в мережі. auth_key_id фактично працює як постійний ідентифікатор пристрою: він не змінюється між сесіями, при зміні IP-адреси, інтернет-мережі або навіть географічного розташування користувача. Це створює технічну можливість для відстеження пристрою тими, хто має доступ до мережевого трафіку, включаючи інтернет-провайдерів, мережевих адміністраторів, державні системи стеження».

«Усі перелічені зловмисники, — йдеться далі в експертизі, — можуть збирати значення auth_key_id за допомогою пасивного спостереження за інтернет-трафіком. Для цього не потрібна складна атака типу "людина посередині" (man-in-the-middle), злом сертифікатів або втручання в роботу протоколу. Достатньо просто перехоплювати мережевий трафік і виконати мінімальну обробку даних.

Оскільки auth_key_id залишається незмінним між сесіями, при зміні мережі та протягом тривалого часу, це створює можливість для довгострокового відстеження пристроїв. Будь-яка структура, що збирає такі ідентифікатори з мережевого трафіку, може створити велику базу даних, пов'язуючи конкретні auth_key_id з місцями підключення до інтернету, часом активності, особливостями трафіку та — якщо особистість користувача відома з інших джерел — з конкретними людьми.

> *Вони [співробітники ФСБ] кажуть: «Ось, нам потрібен о такій-то годині такий-то користувач з IP-адресою. Хто це?» Ми швидко їм відповідаємо*

Така база даних дозволила б, наприклад, відповідати на запитання на кшталт: «Де пристрій з auth_key_id X з'являвся протягом останніх шести місяців?» або «Які пристрої перебували в точці підключення Y у певний період часу Z?». Можливість відстежувати пристрій незалежно від зміни IP-адреси означає, що навіть користувачі, які регулярно змінюють мережі, використовують мобільний інтернет або динамічні IP-адреси, все одно можуть залишатися відстежуваними завдяки постійному auth_key_id», — підкреслюють експерти.

- Як працюють телеграм-вербувальники й боти рашистів, які шукають українців для диверсій

Звідки взялася ця експертиза і до чого тут ФСБ?

Ця експертиза особливо цінна не лише тим, що її провела незалежна компанія з репутацією у сфері кібербезпеки, але й тим, що ініціатором її проведення, судячи з усього, був ніхто інший, як Володимир Веденєєв — один із головних героїв торішнього розслідування «Важливих історій».

У 2025 році нам вдалося з'ясувати, що Веденєєв протягом кількох років обіймав посаду фінансового директора «Телеграму», мав довіреності від компанії та Павла Дурова на підписання документів, а крім того, він обслуговує майже всю мережеву інфраструктуру месенджера в різних країнах світу.

Ми також дізналися, що колишня російська компанія Веденєєва (у 2024 році він переписав її на родича) в рамках секретного держконтракту обслуговує оперативно-розшукові комплекси ФСБ, які використовуються для стеження за громадянами Росії. Але найважливіше — за визнанням самого Веденєєва, за ним закріплений спеціальний куратор із ФСБ — старший офіцер спецслужби, з яким Веденєєв давно співпрацює та ділиться інформацією:

«Мене курує наш фсбівець, сормовський, він намагається, мабуть, погони отримати, тому він усім каже: "Доступ тільки через мене до Володимира". Мені дзвонить, каже: "Слухай, Володь, давай, коротше, там треба якось з ними поспілкуватися з усіма там ними [іншими фєсбівцями], ну і так далі".

Вони [співробітники ФСБ] кажуть: «Ось, нам потрібен о такому-то часу такий-то користувач з IP-адресою. Хто це такий?» Ми розуміємо, що не можемо не відповісти, так? Ми швидко їм відповідаємо. У нас там є авторизовані електронні адреси, з яких вони надсилають запити. Ми швидко їм відповідаємо. Кажемо: «Це там Іванов Іван Іванович, квартира номер 7 там, бла-бла-бла». Вони такі: «Все, окей», — розповідав Веденєєв в інтерв'ю «Важливим історіям».

Після оприлюднення розслідування Веденєєв подав позов до суду у Швейцарії, де він мешкає та має посвідку на проживання, проти головного автора тексту та засновника «Важливих історій» Романа Аніна. У позові Веденєєв не оскаржує твердження з розслідування, але вимагає видалити інтерв'ю, в якому він зізнається у співпраці з ФСБ.

Ознайомлюючись із матеріалами швейцарського судового процесу, ми й виявили ту саму технічну експертизу Symbolic Software, яку додав Веденєєв, мабуть, сподіваючись, що експерти спростують технічні висновки тексту. Однак вони їх підтвердили.

- Як у Телеграмі продають зброю, наркотики, фальшиві кредитки та дитяче порно

Який масштаб цієї проблеми?

«Можливість стежити за користувачами по всьому світу залежить від того, яку частину інтернет-інфраструктури контролює зловмисник. Для справді глобального стеження потрібен доступ до інфраструктури в різних країнах і на різних маршрутах передачі даних», — йдеться в експертизі Symbolic Software.

І саме такий рівень доступу має Володимир Веденєєв. Ось що він, наприклад, говорив в інтерв'ю «Важливим історіям»: «"Телега" не має доступу до дата-центрів ні в Сінгапурі, ні в Маямі: вони жодного разу там не були. Зараз уже побудовано чотири дата-центри. Ми (*компанія GNM, що належить Веденєєву і обслуговує мережеву інфраструктуру "Телеграму". — Р.А.*) у чотирьох уже перебуваємо. <…>

Наразі всі канали зв'язку забезпечую я. Не хтось інший, а саме я! Якщо я дуже захочу, звичайно ж, я можу перекрити цей трафік».

Це зізнання Веденєєва у поєднанні з висновками експерта свідчить про те, що значна частина трафіку «Телеграму» проходить, по суті, через одну людину і:

- цей трафік містить незашифровані ідентифікатори пристроїв, які дають змогу відстежувати користувачів;
- Ця людина має куратора у ФСБ, з яким давно співпрацює та ділиться інформацією.

У минулорічному інтерв'ю «Важливим історіям» Володимир Веденєєв заперечував описану нами вразливість і стверджував, що передає своєму куратору з ФСБ лише інформацію про інтернет-користувачів російських компаній, але не «Телеграму». Чи так це насправді — питання віри.

> *Якщо я дуже захочу, звичайно ж, я можу зняти цей трафік*

Експерт із Symbolic Software зазначає, що вразливість виникла не через якусь технічну недоробку, а внаслідок «фундаментальної відмови "Телеграму" від свого обов'язку захищати приватність користувачів за допомогою сучасних криптографічних механізмів. <…> Рішення проблеми очевидне: «Телеграм» повинен повністю усунути цю вразливість, зробивши обов'язковим використання транспортного шифрування — стандартної технології, яку сьогодні застосовують практично всі великі месенджери. Технічно це реалізується досить просто, майже не впливає на швидкість роботи сервісу, але значно підвищує рівень захисту приватності користувачів. <…>

Доки такі заходи не будуть впроваджені, «Телеграм» несе відповідальність за ризики для конфіденційності, що виникають через те, що постійні ідентифікатори пристроїв залишаються доступними для спостерігачів, які мають доступ до мережевого трафіку», — підсумовує експерт.

- Увага! Нова хвиля фішингових атак у Telegram з використанням історій про жертв війни

Чи дозволяє ця вразливість читати повідомлення?

В експертизі Symbolic Software не йдеться про те, що зловмисники, які мають доступ до трафіку «Телеграму» та ідентифікаторів пристроїв, можуть розшифровувати повідомлення. Однак опитані «Важними історіями» експерти в галузі кібербезпеки такий ризик допускають.

Справа в тому, що ідентифікатор auth_key_id, який «Телеграм» з якихось причин передає по мережі у відкритому вигляді, служить для того, щоб знайти в базі даних ключ конкретного користувача, за допомогою якого месенджер розшифровує повідомлення на своїх серверах. Таким чином, якщо припустити, що у того ж Володимира Веденєєва або іншого пасивного спостерігача за трафіком є доступ до цієї бази, це означає, що вони можуть розшифровувати повідомлення.

Представник «Телеграму» Ремі Вонг (чи існує така людина насправді — невідомо: у мережі немає його фотографій чи інших згадок) надіслав до редакції «Важливих історій» таку відповідь на наш запит: «"Телеграм" відкидає висновки неопублікованого звіту та пов'язані з ним твердження з причин, викладених на цій сторінці.

auth_key_id регулярно змінюється і не розкриває інформацію про користувачів, зміст повідомлень, дані про одержувачів або іншу приватну інформацію. Будь-який спостерігач, здатний бачити цей ідентифікатор, вже мав би доступ до більш надійних способів відстеження, що знаходяться поза контролем «Телеграму». «Телеграм» володіє власною інфраструктурою, яка налаштовується, управляється та контролюється виключно внутрішніми інженерними командами «Телеграму». GNM є шанованим міжнародним інфраструктурним провайдером, ні GNM, ні пан Веденєєв не пов'язані з ФСБ.

- Телеграм-армія Кремля і її шанувальники: зовнішнє інформаційне втручання ефективне, коли воно резонує з реальною незадоволеністю політичною та економічною ситуацією

Також зазначимо, що з 2021 року ані GNM, ні будь-яка інша компанія, пов'язана з паном Веденєєвим, не надавали послуги «Телеграму» у дата-центрі, де зберігається інформація російських та європейських користувачів. Вже один цей факт робить всю теорію змови про зв'язок ФСБ і Веденєєва такою, що не відповідає дійсності».

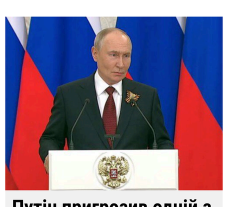
Автор: **Роман Анін**

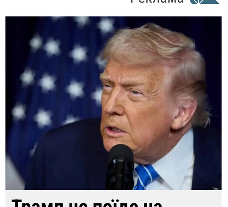
Джерело: **«Важливі історії»**

Like
Tweet

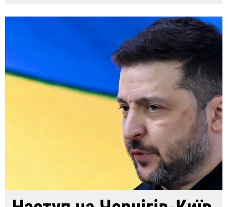
Новини партнерів Реклама

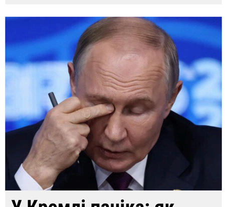
Британська радіостанція повідомила про...


Путін пригрозив одній з країн війною, як...


Трамп не поїде на весілля сина через...

Trump's Secret China Game Is Tearing...


Наступ на Чернігів-Київ з Білорусі: ось...

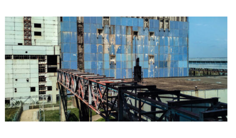

У Кремлі паніка: як Путін зазнає поразки...

Tags: Telegram | війна з Росією | інформаційна безпека | кібербезпека

YOU MAY ALSO LIKE...

Лукашенко готується до втечі? В РФ біля Сочі будують елітну фортецю для білоруського агрофюрера
30 ЖОВТНЯ 2025

Киевский привокзальный криминал: интим за 200 гривен в такси, поборы таксистов и наркосбыт
12 ЛИПНЯ 2011

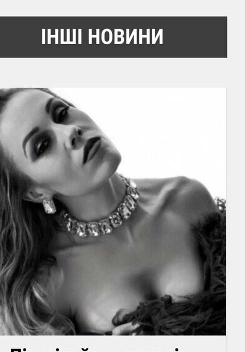

Красти почали вже на етапі підготовки: як «Енергоатом» готується до «Великого атомного будівництва»
2 ЖОВТНЯ 2024

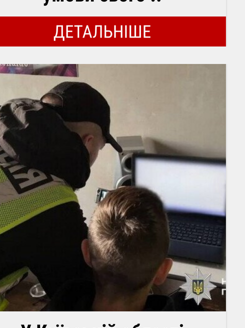
Украина кри... Follow Page

У ФОКУСІ

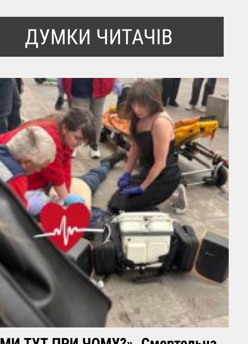
Цифрова ера великого дерибану неоцифрованих метрів або як законно стати безхатьком за три роки на Івано-Франківщині

ІНШІ НОВИНИ

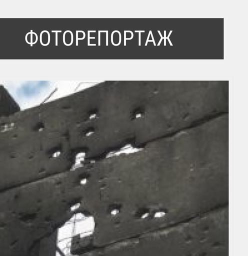

Пів мільйона доларів: Олена Тополя назвала умови свого ..
ДЕТАЛЬНІШЕ


У Київській області викрили підозрюваного у збуті незаконних ..
ДЕТАЛЬНІШЕ

ДУМКИ ЧИТАЧІВ


«А МИ ТУТ ПРИ ЧОМУ?». Смертельна відмова за п'ять хвилин від порятунку та ціна байдужості київської підземки

ФОТОРЕПОРТАЖ


Як виглядає українська ТЕЦ, що пережила не одну ракетну атаку російських загарбників

НОВИНИ IT

Технологии
Загрузка...

Передрук матеріалів "України кримінальної" повністю - з письмового дозволу. Для Інтернет-видань – без обмежень за обов'язкових умов: зазначення адреси ресурсу у вигляді гіперпосилання. Copyright © 2018 Україна кримінальна. Всі права захищені. E-mail для контактів:
cripo@cripo.com.ua