ПУБЛІКАЦІЯ / UK

Іван та Юрій Некуліти, Андрій Нестеренко: сервери, санкції та тіньова сторона хостингу

Опубліковано 15.10.2026 · Оновлено 15.10.2026



У цифрового підпілля є цілком матеріальна сторона: серверні стійки, договори, електроенергія та компанії, які забезпечують зв’язок з інтернетом. У травні 2026 року нідерландські слідчі вилучили понад 800 серверів у справі про ймовірне порушення санкцій. За цією історією стоять брати Іван та Юрій Некуліти, бізнес Stark Industries, зміна корпоративних вивісок та MIRhosting Андрія Нестеренко. KARTEL KHIMPROM зіставив розслідування, реєстри та офіційні документи, щоб з’ясувати, хто за що

відповідав і які питання залишаються відкритими. [1][2]

Коли розслідування доходить до дата-центру

18 травня 2026 року FIOD, нідерландська служба фінансових розслідувань, затримала двох чоловіків — 57-річного з Амстердама та 39-річного з Гааги. Слідчі провели обшуки в комерційних приміщеннях в Енсхеді та Алмері, а також у дата-центрах у Дронтені та Схіпхол-Рейці. Предметом справи стало ймовірне надання економічних ресурсів суб’єктам, що перебувають під санкціями ЄС. [1]

Імена в офіційному повідомленні не наводилися. Журналіст Брайан Кребс назвав затриманих: **Андрій Нестеренко**, пов’язаний із MIRhosting, та **Юсеф Зінад**, пов’язаний із WorkTitans. У його публікації операція розглядається як продовження історії інфраструктури Stark Industries Solutions. [2]

Сенс цієї історії стає зрозумілішим, якщо дивитися далі за кількість вилученої техніки. Злочинний інтернет-сервіс залежить від безлічі постачальників. Один продає обчислювальні потужності, інший надає приміщення, третій підключає обладнання до мережі. Кожен бачить лише свою частину роботи. Для розслідування потрібно відтворити весь ланцюжок, включаючи тих, хто приймав рішення та отримував дохід.

Претензії до провайдера виникають на перетині двох питань: як використовувалася інфраструктура та що було відомо людям, які її надавали. У історії Некуліті та Нестеренко ці питання обговорюються вже кілька років.

Іван Некуліті: від хостингового бізнесу до міжнародного розслідування

У розслідуванні CORRECTIV 2024 року Іван Некуліті постає як підприємець із Бендер, який розбудував бізнес PQ Hosting у Кишиневі. Компанія рекламувала недорогі сервери в багатьох країнах. Для клієнта це виглядало як звичайна комерційна пропозиція: вибрати місце розташування, оплатити ресурси та запустити потрібний сервіс. [3]

Особливе значення мав російський ринок. В інтерв'ю, яке проаналізували журналісти, Іван пояснював переваги закордонних серверів для користувачів, які стикаються з обмеженнями. Іноземна IP-адреса давала змогу виходити в мережу з іншою географічною прив'язкою. Пізніше, відповідаючи на запитання CORRECTIV, він заявив про скорочення діяльності в Росії після початку війни. [3]

Це важливо для розуміння продукту: провайдер продавав доступ до розподіленої інфраструктури. Але відомості про продукт ще не розкривають склад клієнтів. Зв'язки з конкретними зловмисниками дослідники встановлюють за іншими даними — інфраструктурою атак, розміщеними ресурсами та реакцією на повідомлення про порушення.

> **Некуліті Іван**

Історія Івана не обмежується PQ Hosting. У базі даних ICIJ Offshore Leaks є запис про компанію MORENEHOST LTD, де бенефіціаром з 24 квітня 2019 року вказано IVAN NEKULITSY. CORRECTIV пов'язує цей запис із Некуліті. Це історичний корпоративний слід, який дозволяє простежити попередній проєкт; саме володіння офшорною компанією ще не доводить злочину. [4][3]

У квітні 2022 року Morphisec дослідив атаку через вразливість VMware. Аналітики пов'язали сервер одного з етапів завантаження шкідливого коду зі Stark Industries та відзначили зв'язок цієї інфраструктури з PQ Hosting. Такий результат показує, де перебував технічний ресурс. Він не доводить, що власник хостингу сам написав шкідливу програму або керував атакою. [5]

Юрій Некуліті: чому ім'я в реєстрі має значення

Компанію Stark Industries Solutions Ltd зареєстрували у Великій Британії 10 лютого 2022 року. У реєстрі Companies House Іван зазначений як секретар, а Юрій, записаний як Iurie Neculiti, — як директор. У записі про суттєвий контроль Юрій зазначений як власник щонайменше 75% акцій; дата повідомлення — 16 лютого 2024 року. [6][7][8]

У схемі CORRECTIV Юрій був молодшим братом Івана та учасником бізнесу PQ Hosting. При цьому британська компанія Stark формально контролювалася саме ним. Тому історія двох братів вимагає окремого розгляду їхніх ролей: публічний представник бізнесу, директор і зареєстрований власник можуть виконувати різні функції. [3]

> **Некуліті Юрій**

Сам Іван досить докладно пояснював призначення Stark: у відомостях про IP-адреси замість PQ Hosting з’являлася нейтральна назва. За його словами, британська компанія не здійснювала платежів, а допомагала організувати роботу. CORRECTIV розглядав Stark як юридичну ланку бізнесу PQ Hosting. [3]

Для зовнішнього спостерігача це створює кілька рівнів. Назва на сайті, контрагент у документах та організація, зазначена у мережевому ресурсі, можуть не збігатися. Така структура зустрічається й у законному бізнесі. Питання виникає тоді, коли такий розподіл ускладнює встановлення відповідального за ресурс після виявлення зловживання.

Андрій Нестеренко: хто забезпечує підключення

Наступна ланка — MIRhosting. CORRECTIV описував компанію Андрія Нестеренко як одного з мережевих партнерів інфраструктури братів Некуліті. Нестеренко підтвердив журналістам, що Stark Industries є клієнтом. У тій самій публікації зазначалося, що у 2014–2016 роках він працював торговим представником компанії Serverius. [3]

У Нестеренко є й інша публічна професійна біографія. MIRhosting повідомляє про його виступ на фортепіанному конкурсі в Енсхеді у 2002 році, другу премію та подальше навчання у Михайла Маркова. Компанія розповідає про багаторічне технічне супроводження конкурсу. Ці відомості характеризують його кар’єру; вони не підтверджують і не спростовують претензій до хостингового бізнесу. [9]

> **Нестеренко Андрій Володимирович**

Головне питання до MIRhosting пов’язане з характером послуг, що надаються. У травні 2026 року компанія пояснила, що забезпечувала WorkTitans розміщення обладнання, електроживлення та мережеве підключення. Управління апаратурою, програмами та даними, за її заявою, залишалося за клієнтом. [10]

Це принципова відмінність. Проходження трафіку через мережу саме по собі не доводить управління клієнтським сайтом. Для оцінки обізнаності постачальника важливими є конкретні повідомлення, їхній зміст, терміни реагування та подальші дії. Окреме питання — кому надавалися послуги та ресурси в період дії санкцій.

Кілька компаній — кілька різних функцій

Щоб не плутати учасників, корисно розкласти опубліковані зв’язки за ролями. Таблиця відображає відомості за різні роки і не є переліком чинних договорів на сьогодні.

Структура	Роль у опублікованій історії	Підстава
PQ Hosting	Хостинг-бізнес братів Некуліті, описаний у розслідуванні 2024 року.	CORRECTIV [3]

Структура	Роль у опублікованій історії	Підстава
Stark Industries Solutions Ltd	Британська юридична особа, пов’язана з мережевою інфраструктурою бізнесу.	Companies House; CORRECTIV [6][3]
PQ Hosting Plus S.R.L.	Організація, щодо якої аналітики зафіксували перенесення AS44477 у травні 2025 року.	Recorded Future [11]
WorkTitans B.V. / THE.Hosting	Компанія та бренд, що фігурують у подальшій історії перенесення послуг.	Recorded Future [11]
MIRhosting	Мережеве підключення; компанія також надавала послуги розміщення обладнання для WorkTitans.	Заява MIRhosting [10]
Serverius	Оператор дата-центру, про якого йдеться у розслідуванні CORRECTIV.	CORRECTIV [3]

З таблиці не випливає, що всі перелічені структури мають однаковий правовий статус. Вона показує, чому розслідування діяльності конкретного сервісу не можна завершувати на першій назві, знайденій у мережевому довіднику.

Що було виявлено на серверах: пропаганда, DDoS-атаки та фінансова кіберзлочинність

CORRECTIV детально аналізував ресурс RRN, пов’язаний з інформаційною кампанією Doppelganger. За висновками журналістів, він працював через інфраструктуру братів Некуліті в Нідерландах. Після запитань видання Іван повідомив про блокування відповідного облікового запису та сервера. Однак CORRECTIV вважав, що ресурс продовжував використовувати пов’язану інфраструктуру, вже приховану додатковим сервісом. [3]

У тому ж розслідуванні розглядалася NoName057(16), відома своїми DDoS-атаками. CORRECTIV навів спостереження Spamhaus: із 48 виявлених керуючих скриптів за два місяці на початку 2024 року половина перебувала на серверах Stark. Ця повторюваність стала однією з підстав для запитань до провайдера. Іван заперечував можливість атак і стверджував, що компанія серйозно ставиться до скарг. [3]

Подальші дослідження розширили картину. Recorded Future повідомляв, що в середині 2025 року інфраструктуру Stark використовував GrayAlpha — кластер, який значною мірою перетинається з фінансово мотивованою групою FIN7. Таким чином, коло описаних загроз включало не лише політичні операції. [11]

Загальний комерційний постачальник може обслуговувати різні, не пов’язані між собою групи. Для аналізу це важливе застереження: сусідство ресурсів в одній мережі ще не означає спільного керівництва. Але повторюване використання одного постачальника різними зловмисниками робить його практику роботи з клієнтами самостійним предметом суспільного інтересу.

Санкції оголошено, інфраструктура змінюється

20 травня 2025 року Рада ЄС ввела санкції проти Stark Industries Solutions, Івана та Юрія Некуліті. В офіційному повідомленні як підстава зазначено підтримку дестабілізуючих дій суб’єктів, пов’язаних із Росією, зокрема інформаційних операцій та кібератак. Ці заходи передбачають заморожування активів та обмеження на надання коштів і ресурсів. [12]

Технічне дослідження Recorded Future описує зміни, що почалися ще до оголошення санкцій. 16 травня 2025 року аналітики зафіксували перенесення AS44477 на PQ Hosting Plus S.R.L. Потім з’явилися бренд THE.Hosting під WorkTitans B.V. та нова автономна система AS209847. Дослідники оцінили цю перебудову як ймовірну спробу зберегти послуги при зміні юридичних та мережевих позначень. [11]

Автономна система — це мережа під єдиним технічним управлінням, яку інші мережі розпізнають за номером. Зміна такої реєстрації може мати більший вплив, ніж зміна логотипу: вона стосується того, як інфраструктура представлена іншим операторам. При цьому призначення конкретної зміни визначається за сукупністю обставин, а не за одним новим номером.

16 вересня 2025 року британська компанія Stark Industries Solutions Ltd отримала в Companies House статус «Dissolved» (ліквідована). Це факт щодо юридичної особи. Він не дає відповіді на питання, що сталося з обладнанням, даними клієнтів та послугами, які раніше були пов’язані з компанією. [6]

Документ від 8 жовтня 2026 року: що тепер затверджує Рада ЄС

В оновлених санкційних записах щодо братів Некуліті Рада ЄС описала перенесення інфраструктури Stark до WorkTitans B.V., яку названо прикривною структурою, та роль MIRhosting у забезпеченні підключення. Іван та Юрій вказані як бенефіціари цієї конструкції. За оцінкою Ради, вона відображала спробу приховати власність та зберегти хостингові послуги під новими юридичними та мережевими позначеннями. [13]

Це вже офіційна оцінка щодо санкцій, яка виходить за межі попередніх журналістських припущень. Однак вона не замінює кримінального вироку кожній особі чи компанії, згаданим в описі. Зокрема, згадка про MIRhosting у записах братів не є рівнозначною персональним санкціям проти Нестеренко.

При порівнянні матеріалів видно, як змінюється предмет публічного обговорення: від окремих ресурсів на серверах — до збереження контролю над інфраструктурою після введення обмежень. Саме спадкоємність бізнесу стає центральним питанням цієї історії.

Заперечення MIRhosting: суперечка щодо походження атак

Нестеренко повідомив KrebsOnSecurity, що перехід обладнання та клієнтського портфеля до WorkTitans відбувся до введення санкцій і не мав на меті їх обхід. Він заперечив підтримку кіберзлочинності. Компанія оголосила про тимчасове призупинення послуг WorkTitans та співпрацю з владою. [2][10]

2 червня 2026 року MIRhosting опублікувала власний аналіз трафіку за жовтень–листопад 2025 року. За її даними, усі 4 468 виявлених DDoS-аномалій були вхідними: ціллю були адреси, що обслуговуються. Компанія стверджувала, що її спостереження не вказують на вихідні атаки. [14]

При цьому MIRhosting зазначила обмеження: збережена деталізація деяких вимірювань сама по собі не виключає короткочасних сплесків. Компанія пообіцяла надати вихідні дані компетентним органам. Під час підготовки цього матеріалу весь масив даних не перевірявся незалежно. [14]

Суперечка щодо напрямку атак та питання дотримання санкцій вимагають різних доказів. Навіть вичерпна відповідь щодо трафіку за конкретний тиждень не дозволить автоматично встановити, хто контролював компанію-одержувача послуг. І навпаки, корпоративний зв’язок сам по собі не доводить запуск атаки з конкретного сервера.

У перевірених матеріалах немає підтвердження обвинувального вироку Нестеренко у описаній справі. Його поточний запобіжний захід також не встановлено: повідомлення про затримання у травні не дозволяє стверджувати, що він залишається під вартою у жовтні.

Де в цій історії з’являється «Хімпром»

Для редакції KARTEL KHIMPROM вивчення інфраструктури є важливим як частина роботи над цифровими сервісами, якими можуть користуватися злочинні мережі. Але в цьому кейсі зв’язок із конкретним картелем вимагає особливо точного формулювання.

У звіті Intrinsec *Від шпигунства до психологічних операцій* проаналізовано кампанії UAC-0050 та UAC-0006. На сторінці 11 наведено текст погроз, відправник яких дякує «Хімпрому» та адміністрації Rutor. В інших розділах дослідники розглядають маршрутизацію та інфраструктурні перетини, пов’язані зі Stark та MIRhosting. [15]

Згадка про картель зроблена самим автором погроз. Це не підтверджене свідчення від його імені і не доказ угоди між картелем та провайдером. Чужа назва може використовуватися для залякування, створення хибного сліду або самореклами. Причину такого згадування необхідно встановлювати окремо.

Тому наявні матеріали дають змогу досліджувати перетин тем — злочинних сервісів, загроз та постачальників інфраструктури, — але не оголошувати Некуліті чи Нестеренко учасниками «Хімпрому». Документів про безпосереднє обслуговування картелю, його платежі цим особам або їхні особисті домовленості з Єгором Буркіним у вивчених джерелах немає.

Для продовження цієї частини перевірки потрібен конкретний зв’язуючий факт: встановлена приналежність сервісу, підтверджений постачальник у відповідний період, договір або платіж. Виявлення схожих назв у різних розслідуваннях є недостатнім.

Чому історія важливіша за одну вивіску

Сильна сторона цього кейсу — можливість зіставити кілька типів доказів. Корпоративний реєстр показує формальні ролі. Технічне дослідження відстежує зміни в мережі. Слідчий звіт описує підстави операції. Санкційний акт викладає позицію Ради ЄС. Відповіді компанії дозволяють перевірити, що саме вона оскаржує.

Кожне джерело відповідає на свою частину питання. Разом вони дають більш змістовну картину, ніж перелік гучних імен. Але й разом не звільняють від необхідності доводити кожен особистий зв’язок.

Головне питання, що залишається відкритим, — хто фактично зберігав можливість керувати інфраструктурою та отримувати від неї дохід після корпоративних змін. Відповідь вимагає інформації про контроль, передачу активів та реальне виконання договорів. Саме вони дозволяють відрізнити звичайний продаж бізнесу від схеми, що зберігає інтереси колишніх власників.

Коли злочинний сервіс зникає з однієї адреси, важливо зрозуміти, чи зникла його технічна та фінансова основа. Історія Stark, братів Некуліті та MIRhosting показує, чому таке розслідування має продовжуватися за межами сайту та його логотипу — аж до компаній, обладнання та людей, які приймають рішення.

Матеріал підготовлено на основі відкритих документів та опублікованих розслідувань, перевірених станом на 15 жовтня 2026 року. Висновки відомств та дослідників наведено з посиланням на джерела. Позиції фігурантів викладені на основі їхніх опублікованих відповідей; редакція не подає ці відповіді як отримані на власні запити.

Джерела

1. FIOD — два затримання та вилучення понад 800 серверів у справі про санкції, 22.05.2026
   https://www.fiod.nl/fiod-houdt-twee-verdachten-aan-wegens-overtreding-sanctiewetgeving/
2. KrebsOnSecurity — затримання Андрія Нестеренко та Youssef Zinad, 25.05.2026
   https://krebsonsecurity.com/2026/05/netherlands-seizes-800-servers-arrests-2-for-aiding-cyberattacks/
3. CORRECTIV — розслідування про братів Некуліті, PQ Hosting, Stark та MIRhosting, 31.05.2024
   https://correctiv.org/en/fact-checking-en/2024/05/31/hacks-and-propaganda-meet-the-two-brothers-bringing-russias-cyber-war-to-europe/
4. ICIJ Offshore Leaks / Pandora Papers — MORENEHOST LTD та бенефіціар ІВАН НЕКУЛІЦЬКИЙ
   https://offshoreleaks.icij.org/nodes/240120865
5. Morphisec Labs — дослідження атаки через вразливість VMware та інфраструктури Stark, 25.04.2022
   https://www.morphisec.com/blog/vmware-identity-manager-attack-backdoor/

6. Companies House — Stark Industries Solutions Ltd, № 13906017; статус та дати реєстрації
https://find-and-update.company-information.service.gov.uk/company/13906017

7. Companies House — посадові особи Stark Industries Solutions Ltd
https://find-and-update.company-information.service.gov.uk/company/13906017/officers

8. Companies House — особи, які мають значний контроль над Stark Industries Solutions Ltd
https://find-and-update.company-information.service.gov.uk/company/13906017/persons-with-significant-control

9. MIRhosting — біографічні відомості про Андрія Нестеренко та співпрацю з фортепіанним конкурсом, 22.02.2026
https://mirhosting.com/mirhosting-international-piano-competition-enschede-livestream

10. MIRhosting — заява у відповідь на публікації ЗМІ, 22.05.2026
https://mirhosting.com/verklaring-mirhosting-naar-aanleiding-van-recente-mediapublicaties

11. Recorded Future / Insikt Group — One Step Ahead: Stark Industries Solutions випереджає санкції ЄС, 27.08.2025
https://www.recordedfuture.com/research/one-step-ahead-stark-industries-solutions-preempts-eu-sanctions

12. Рада ЄС — санкції проти Stark Industries та братів Некуліті, 20.05.2025
https://www.consilium.europa.eu/en/press/press-releases/2025/05/20/russian-hybrid-threats-eu-lists-further-21-individuals-and-6-entities-and-introduces-sectoral-measures-in-response-to-destabilising-activities-against-the-eu-its-member-states-and-international-partners/

13. Рада ЄС — Регламент 2026/2257 від 08.10.2026, пункти 27–28; офіційний текст у BOE
https://www.boe.es/buscar/doc.php?id=DOUE-L-2026-81528

14. MIRhosting — власний аналіз трафіку за жовтень–листопад 2025 року, опубліковано 02.06.2026
https://mirhosting.com/the-november-2025-danish-election-attacks-what-our-own-network-data-shows

15. Intrinsec — Від шпигунства до психологічних операцій: Відстеження операцій та надійних постачальників UAC у 2025 році; с. 11, 18, 25–26
https://www.intrinsec.com/wp-content/uploads/2025/10/TLP-CLEAR-From-espionage-to-PsyOps-Tracking-operations-and-infrastructure-of-UACs-in-2025-EN.pdf

Використання матеріалів

У разі використання матеріалів обов’язкове активне посилання на оригінальну публікацію.

Оригінал матеріалу

https://kartel-khimprom.com/uk/article/ivan-ta-yurij-nekuliti-andrij-nesterenko-serveri-sankczi%d1%97-ta-tinova-storona-hostingu/