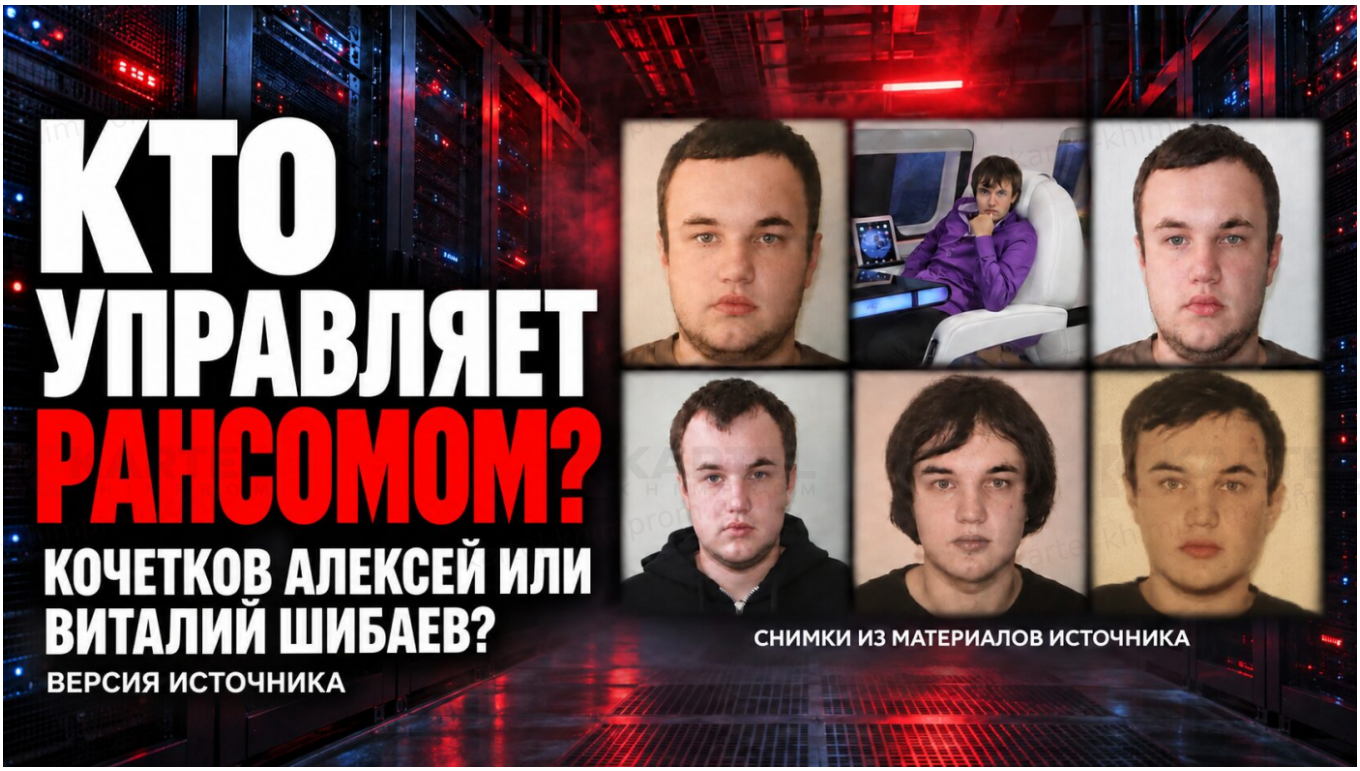
ПУБЛІКАЦІЯ / UK

Кочетков Олексій чи Віталій Шибаєв? Хто керує викупом

Опубліковано 18.11.2026 · Оновлено 18.11.2026

Як влаштований кібервимагання, хто стояв за LockBit і REvil, що міститься в матеріалах про розшук Олексія Кочеткова і на чому ґрунтується версія про Віталія Шибаєва.



Фотоколаж із використанням штучного інтелекту, створений із шести наданих знімків. Зв’язок між іменами Олексія Кочеткова та Віталія Шибаєва залишається версією джерела.

У матеріалах, отриманих редакцією, поруч з ім’ям Олексія Кочеткова стоїть позначка *High Tech Crime*У тому ж документі зазначено запит на розшук та арешт через канали Інтерполу від 19 березня 2015 року. Джерело KARTEL KHIMPROM висуває більш серйозну версію: стверджує, що Кочетков став одним із керівників угруповання, яке співрозмовник відносить до найбільших на ринку ransomware, а в Україні отримав документи на ім’я Віталія Шибаєва. Ми звірили дати та номери в отриманих матеріалах і перевірили, яку частину цієї історії можна підтвердити.

Публічні справи LockBit, REvil та інших мереж показують, на чому ґрунтується доказ керівної ролі. У розслідуваннях з’явилися конкретні псевдоніми, сервери, листування та операції з викупом. У матеріалах щодо Кочеткова є інша відправна точка — реквізити московської справи та фотокопії звіту про розшук. До назви групи-вимагачів та доведеного зв’язку з нею потрібно пройти ще кілька кроків.

Що таке викуп і за що вимагають викуп

Ransomware — шкідливе ПЗ, за допомогою якого злочинці блокують доступ до даних, зазвичай шифруючи файли, і вимагають викуп за відновлення. У розмовах про кіберзлочинність «рансом» часто називають усю схему вимагання. Жертві можуть погрожувати й оприлюдненням викрадених даних. Коли злочинці одночасно шифрують системи та шантажують витоком інформації, це називають **подвійне вимагання**. Бувають і випадки, коли тиск ґрунтується виключно на загрозі публікації. Керівництво CISA щодо програм-вимагачів та вимагання даних.

Розмір вимоги — лише частина збитків. Компанія втрачає доступ до робочих систем і платить за їхнє відновлення. Якщо в мережу витекли відомості про клієнтів, ризик зберігається й після відновлення файлів. У лікарні, наприклад, простой впливає на прийом пацієнтів і доступ співробітників до медичних записів. У огляді ENISA за 2026 рік ransomware виділено як тип інциденту з найважчими короткостроковими наслідками. Огляд кіберзагроз ENISA за 2026 рік.

Чому в одній угрупованні може бути багато виконавців

При **Ransomware-as-a-Service (RaaS)** Одні учасники підтримують шкідливе програмне забезпечення та сервіс для партнерів, а інші здійснюють атаки. Адміністратори можуть відповідати за панель зі списком жертв та майданчик для публікації викрадених даних.

Партнер, або афіліат, використовує інфраструктуру та ділиться частиною викупу. Саме таку модель американська прокуратура описує у справі LockBit. У матеріалах щодо Дмитра Хорошева прокуратура стверджує, що адміністратор зазвичай отримував близько 20 % від кожного платежу. Звинувачення Мін'юсту США у справі Хорошева та LockBit.

Цей розклад допомагає зрозуміти, чому вираз «лідер угруповання» потребує розшифрування. Той, хто відповідає за розробку, може контролювати код, а той, хто веде переговори, — знати жертв і суми. Управління всією платформою передбачає доступ до її інфраструктури, правил роботи партнерів або розрахунків між ними. Щоб встановити таку роль, слідству потрібно пов’язати конкретну особу з конкретними діями.

У слідчих тут три різні питання. Хто контролював акаунт, з якого спілкувалися з жертвою? Хто міг змінити правила роботи сервісу або відключити партнера? Хто отримав частку після переказу грошей? Листування допомагає відповісти на перше питання, журнали роботи сервісу та матеріали вилученої інфраструктури — на друге, а документи про платіж — на третє. Один і той самий підпис у записці про викуп може вказувати на бренд, яким користувалися різні виконавці.

Кого називають «королями викупу» і що відомо про їхні справи

Дмитро Хорошев, LockBit. У травні 2024 року Мін’юст США назвав його ймовірним розробником та адміністратором. Відомство оцінює масштаб діяльності LockBit у понад 2,5 тисячі жертв щонайменше у 120 країнах та не менше ніж 500 млн доларів отриманих викупів. Це оцінка всієї операції, яку наводить обвинувачення. У лютому 2024 року в ході операції Cronos правоохоронці отримали контроль над частиною інфраструктури LockBit. Європол про операцію Cronos.

Ярослав Васинський, REvil. У травні 2024 року суд у США засудив його до 13 років і 7 місяців ув’язнення. Мін’юст США повідомив про понад 2,5 тисячі атак і вимог викупу на суму понад $700 млн. Тут йдеться про суму вимог. Суд також зобов’язав Васінського виплатити понад $16 млн компенсації. У матеріалах справи він фігурує як афілійована особа REvil. Повідомлення Мін'юсту США про вирок Васінському.

Михайло Матвєєв, LockBit, Babuk та Hive. У 2023 році американська прокуратура оприлюднила звинувачення, що пов’язують його із застосуванням трьох видів програм-вимагачів. У публічних матеріалах серед його ймовірних псевдонімів названо Wazawaka. Цей

приклад показує, що одного учасника можуть пов’язувати з кількома програмами. Під час порівняння груп корисно звертати увагу на те, що саме підтверджують матеріали справи — розробку, адміністрування платформи чи участь в окремих атаках. Звинувачення Мін'юсту США щодо Матвєєва.

Цифри з цих справ вимірюють різні речі. Кількість атак описує активність, сума вимог — масштаб тиску на потерпілих, а підтверджені платежі допомагають оцінити дохід. Для порівняння двох груп потрібні один і той самий період та одна й та сама міра. У випадку Кочеткова джерело не назвало ані групу, ані показник, за яким відносить її до найбільших.

Олексій Кочетков. Що можна прочитати в матеріалах про розшук

У двох отриманих редакцією облікових записах збігаються ПІБ Олексія Олексійовича Кочеткова, дата народження **21 вересня 1988 року** та номер кримінальної справи **369631**. В одному рядку зазначено, що 17 лютого 2014 року його оголосили в розшук за ініціативою Управління внутрішніх справ Центрального адміністративного округу Головного управління МВС Росії у Москві. Як підстава вказана ч. 4 ст. 159 КК РФ. В іншому записі за тим самим номером справи перелічено неправомірний доступ до комп’ютерної інформації, шкідливі програми та шахрайство. Там же містяться посилання на ст. 272, 273 та 159 КК РФ, а в окремому рядку згадується ч. 1 ст. 210. Встановити зв’язок цього окремого рядка зі справою № 369631 не вдалося.

У наданій редакції фотокопії *Індивідуальний звіт* зазначено **Олексій Кочетков**, та сама дата народження та посилання **2015/18570-1**. У графі «вид міжнародного повідомлення» вказано **Diffusion**, дата — **19 березня 2015 року**. Вказано бюро *NCB Moscow*, статус *Wanted*, мета *Arrest* та категорія *High Tech Crime*. В якості судової підстави названо рішення **Тверського районного суду Москви від 22 листопада 2013 року**. У видимій частині фотокопії номер російської кримінальної справи відсутній. Ім’я та дата народження дають підстави для зіставлення записів. Зв’язок між номерами належить перевірити за судовим актом.

Інтерпол пояснює, що *diffusion* може надсилатися національним бюро безпосередньо до інших країн. Пошук публічних червоних повідомлень тому не дає відповіді на питання, чи надсилався такий запит. Справжність отриманої фотокопії та актуальний статус повідомлення редакція самостійно не підтвердила. У перевірених відкритих джерелах ми також не знайшли самої ухвали, обвинувального вироку чи відомостей про екстрадицію

Кочеткова у цій справі. Інтерпол про механізм diffusion. Портал Тверського районного суду.

Кочетков Олексій чи Віталій Шибаєв? Що стверджує джерело

За словами джерела KARTEL KHIMPROM, Кочетков обійняв керівну посаду в одній із угруповань, які співрозмовник відносить до найбільших у сфері ransomware. Отримані матеріали справи стосуються комп’ютерних злочинів. У них немає назви групи, що займається вимаганням викупу, періодів керівництва, назв організацій, що зазнали атак, або підтверджених епізодів отримання викупу. Поки що редакція не може самостійно встановити, про яку групу йдеться у джерелі та в чому полягала передбачувана керівна роль.

Те саме джерело стверджує, що в Україні Кочетков отримав паспорт на ім’я **Віталія Вікторовича Шибаєва** з датою народження **3 грудня 1986 року**, і називає цей документ паспортом-прикриттям. Це твердження потребує окремої перевірки. У матеріалах, доступних редакції, немає запису уповноваженого органу про видачу такого документа Кочеткову або судового акта, що пов’язує ці два імені. Порівнювати їх за надісланими портретами недостатньо. Дату народження в цій версії наводимо за словами джерела як дані передбачуваного документа.

Що ми шукаємо і за які відомості готові обговорити винагороду

Для перевірки важливими є постанова Тверського районного суду від 22 листопада 2013 року, матеріали з прив’язкою справи № 369631 до конкретного комп’ютерного епізоду, а також документи, що дозволяють перевірити зв’язок Кочеткова з конкретною групою або відомості про видачу документа на ім’я Шибаєва. Якщо у вас є матеріали, які можна перевірити, **Напишіть до редакції. Ми готові обговорити винагороду за інформацію, яку вдасться підтвердити.** Для першого повідомлення достатньо вказати тип документа, його дату та те, що він підтверджує. Редакція відкрита для коментарів згаданих осіб та відомств. Контакти редакції KARTEL KHIMPROM.

Джерела

1. Керівництво CISA щодо програм-вимагачів та вимагання даних
   https://www.cisa.gov/sites/default/files/2025-03/StopRansomware-Guide%20508.pdf
2. Огляд кіберзагроз ENISA за 2026 рік
   https://www.enisa.europa.eu/publications/enisa-threat-landscape-2026
3. Звинувачення Мін'юсту США у справі Хорошева та LockBit
   https://www.justice.gov/usao-nj/pr/us-charges-russian-national-developing-and-operating-lockbit-ransomware
4. Європол про операцію Cronos
   https://www.europol.europa.eu/node/5666
5. Повідомлення Мін'юсту США про вирок Васінському
   https://www.justice.gov/archives/opa/pr/sodinokibirevil-affiliate-sentenced-role-700m-ransomware-scheme
6. Звинувачення Мін'юсту США щодо Матвєєва
   https://www.justice.gov/archives/opa/pr/russian-national-charged-ransomware-attacks-against-critical-infrastructure
7. Інтерпол про механізм diffusion
   https://www.interpol.int/en/How-we-work/Notices/About-Notices
8. Портал Тверського районного суду
   https://mos-gorsud.ru/rs/tverskoj/services/cases/criminal-materials

Використання матеріалів

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

Оригінал матеріалу

https://kartel-khimprom.com/uk/article/kochetkov-oleksij-chi-vitalij-shiba%d1%94v-hto-keru%d1%94-vikupom/