Конвеєр фейків та спаму: як білоруська платформа ProxySmart допомагає шахраям орендувати тисячі «українських» номерів

Читать на русском

Конвеєр фейків та спаму: як білоруська платформа ProxySmart допомагає шахраям орендувати тисячі «українських» номерів

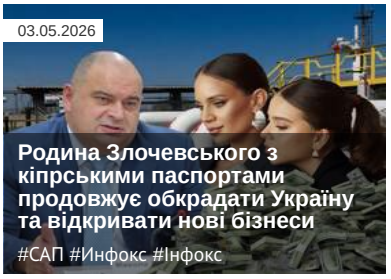
Ваша «сестра» у відчаї просить терміново переказати гроші — ось тільки сестри у вас немає. Докучливі «страхові агенти», фальшиві дзвінки від імені оператора зв'язку, тривожні SMS із вимогою негайно перейти за посиланням — усе це давно стало частиною повсякденного життя. А за переважною більшістю таких атак стоять SIM-ферми: стелажі з мобільними телефонами та модемами, здані в оренду шахраям для автоматизованих кампаній у глобальному масштабі.

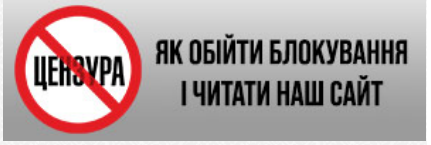
Те, що SMS-повідомлення надійшло з місцевого номера, зовсім не означає, що його надіслав хтось із вашої країни. Саме доступ до місцевої телеком-інфраструктури ініціатори загроз і використовують, аби вселити довіру до підроблених звернень, зазначає видання Cybercalm. У квітні 2026 року компанія Infrawatch оприлюднила результати масштабного розслідування, що показує, як ціла індустрія «SIM-ферм як послуги» живить шахрайство по всьому світу — зокрема й в Україні.

Що таке SIM-ферма і чому вона небезпечна

SIM-ферма — це мережа з сотень, а іноді й тисяч SIM-карток, підключених до модемів та смартфонів, які одночасно виконують обчислювальні й комунікаційні завдання. За логікою вона нагадує криптоферму: велика кількість уніфікованого обладнання, орієнтованого на автоматизацію. Проте замість видобутку криптовалюти SIM-ферма продукує телефонні номери та мобільні IP-адреси «на вимогу».

Важливі новини





Останні новини

По датi | По переглядам | По коментарям

00:03 Тайвань, Іран та РФ на порядку денному: Трамп летить до Китаю для складних переговорів із Сі Цзіньпіном

10 травня 2026 г.

23:56 Повторення «югославського сценарію»: У Євросоюзі готуються до сплеску нелегального обігу зброї

23:49 «Мені це не подобається!»: Трамп різко відреагував на пропозиції Тегерана

23:43 **Російські війська просунулися західніше Гришиного на Покровському напрямку, – DeepState**

23:36 30 днів на переговори: Тегеран пропонує США припинити вогонь та частково вивезти уран в обмін на зняття санкцій

Сам собою такий пристрій не є злочинним інструментом. Бізнес використовує SIM-ферми для тестування та масштабування телеком-сервісів, розробники — для перевірки мобільних застосунків, компанії — для легальних масових розсилок. Але коли керування цією інфраструктурою переходить до зловмисників, вона перетворюється на потужний конвеєр спаму, смішингу (фішингу через SMS), шахрайських дзвінків та автоматизованих атак на онлайн-сервіси.

Кожна SIM-картка у фермі фактично є окремим «пристроєм», з якого можна реєструвати нові облікові записи, обходити SMS-верифікацію, керувати бот-мережами в соцмережах і на форумах, поширювати дезінформацію та пропаганду, а також маскувати справжнє походження трафіку. Саме тому SIM-ферми стали улюбленим інструментом організованої кіберзлочинності: вони дають злочинцям «місцеве обличчя» у будь-якій країні — американський номер для атак на мешканців США, німецький — на користувачів у Німеччині, український — для атак на українців.

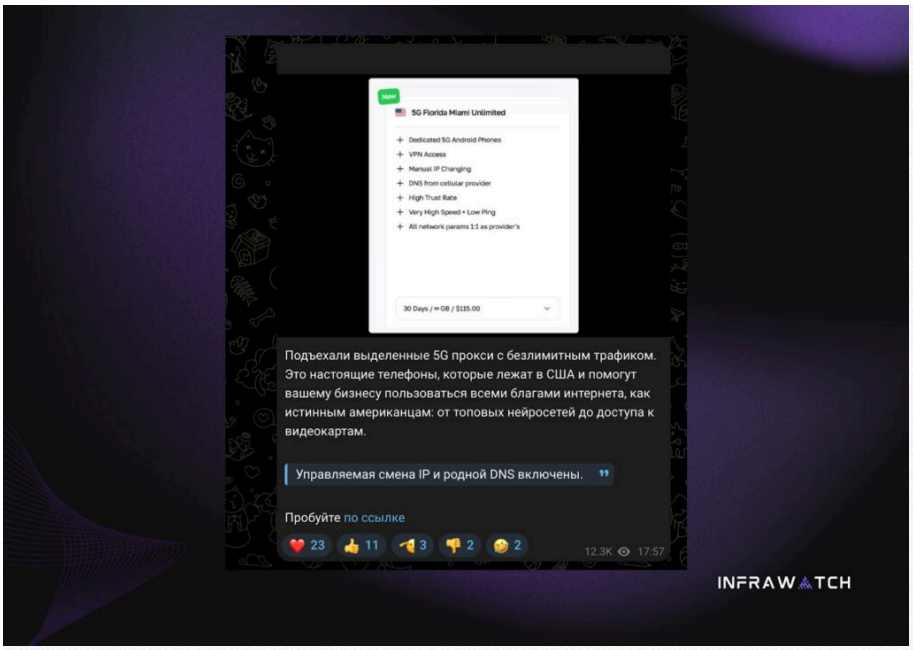
Серйозну загрозу бачать і державні органи. Секретна служба США попередила, що масштабні SIM-ферми здатні не лише розсилати шахрайські повідомлення, а й перевантажувати мобільні мережі, створювати перешкоди у роботі служб екстреного виклику та слугувати каналом для зашифрованих комунікацій організованих злочинних угруповань.

94 локації у 17 країнах: як виглядає «SIM-ферма як послуга»

Розслідування Infrawatch, оприлюднене у квітні 2026 року, відкрило цілу екосистему комерційних SIM-ферм, об'єднаних спільною платформою керування ProxySmart. За даними компанії, йдеться про 87 активних панелей керування у 17 країнах та щонайменше 94 фізичні локації зі стелажами телефонів і 4G/5G-модемів, підключених до мереж місцевих операторів. Найбільша концентрація обладнання — у США, де ферми виявлено у 19 штатах; окремі майданчики зафіксовано у Європі, Південній Америці та Австралії.

Країнами, де знайдено фізичну інфраструктуру, стали США, Канада, Велика Британія, Німеччина, Іспанія, Португалія, Україна, Латвія, Франція, Румунія, Бразилія, Ірландія, Нідерланди, Австралія, Італія, Польща та Грузія. Ферми підключені щонайменше до 35 мобільних операторів, серед яких AT&T, Verizon, T-Mobile, Vodafone, EE, O2, Three, Deutsche Telekom, Orange, Rogers, Telstra, а також українські Kyivstar і lifecell. Доступом до цієї інфраструктури торгує щонайменше 24 комерційних провайдерів проксі-сервісів.

Саму платформу ProxySmart дослідники пов'язують із розробниками з Мінська (Білорусь). Вона продається як «коробкове рішення»: власнику ферми пропонують вебінтерфейс, API, автоматичну ротацію IP-адрес (зокрема шляхом вмикання-вимикання «режиму польоту» на кожному телефоні), підтримку протоколів OpenVPN, SOCKS5, VLESS та HTTP-проксі, а також функцію підміни відбитків операційної системи — пристрій може видавати себе за macOS, iOS, Windows чи Android. Сервіси, що працюють на базі ProxySmart, активно рекламуються на Telegram-каналах, орієнтованих на російськомовну аудиторію, — зокрема як спосіб обійти геоблокування та отримати доступ до «західних» AI-сервісів і платформ для роботи з GPU.



Показово, що жодних реальних перевірок клієнтів (KYC) більшість провайдерів не проводить, а оплату часто приймають у криптовалюті. Це означає, що фактично будь-який покупець — включно з професійними шахраями та операторами бот-мереж — може орендувати готову інфраструктуру для атак.

Реакція правоохоронців: від Нью-Йорка до операції SIMCARTEL

У вересні 2025 року Секретна служба США демонтувала у Нью-Йорку мережу з понад 300 SIM-серверів і близько 100 000 SIM-карток, що працювала поблизу штаб-квартири ООН. За оцінкою правоохоронців, потужності цієї ферми вистачило б, аби вивести з ладу мобільний зв'язок у масштабах усього Нью-Йорка. Місяцем пізніше, у жовтні 2025 року, Європол підтримав міжнародну операцію SIMCARTEL в Австрії та Латвії: сім затриманих, 1200 вилучених SIM-боксів і 40 000 активних SIM-карток, які фігурують щонайменше у 1700 кримінальних провадженнях про кібершахрайство.

Попри гучні ліквідації, SIM-ферми залишаються у так званій «сірій зоні» законодавства більшості країн. Саме обладнання не є забороненим, а регулятори зазвичай не мають інструментів, щоб оперативно реагувати на зміну власника чи «орендаря» інфраструктури. Наразі єдиною державою, яка на рівні закону заборонила володіння та постачання SIM-ферм, залишається Велика Британія — там нова норма покликана позбавити шахраїв готового інструменту для масових атак. Проте поза межами юрисдикції Лондона ця заборона не діє.

Що це означає для українців

Україна є однією з 17 країн, де Infrawatch зафіксувала фізичні SIM-ферми, а також однією з юрисдикцій, до яких активно маршрутизується шахрайський трафік. За даними Департаменту кіберполіції Національної поліції України, смішинг і фішингові SMS стабільно входять до топу онлайн-загроз: користувачі отримують повідомлення про «заблоковану картку», «недоставлену посилку», «державну субсидію», «виграш» або нібито від знайомого з проханням позичити гроші. Лише у 2024 році середня сума шахрайської транзакції з платіжними картками в Україні зросла на 40% і сягнула понад 4200 гривень, а сумарні збитки перевищили мільярд гривень.

Додатковий ризик створює російсько-українська війна. Росія та її проксі-структури мають очевидний інтерес до інфраструктури, яка дозволяє розсилати SMS і здійснювати дзвінки з «українських» номерів — для поширення паніки, дезінформації, фейкових звернень від імені військових, волонтерів чи держорганів. Той факт, що платформа ProxySmart розроблена у Мінську та активно просувається у російськомовному сегменті, не додає оптимізму.

Як розпізнати атаку через SIM-ферму і не стати жертвою

Жоден технічний захід не скасовує основного правила: дзвінки та SMS варто сприймати критично незалежно від того, з якого номера вони надійшли. Місцевий код країни чи оператора більше не є гарантією, що повідомлення справжнє.

- Не довіряйте знайомому вигляду номера. SIM-ферми дають шахраям саме локальну «прописку». Повідомлення з українського номера цілком може бути частиною автоматизованої кампанії, розгорнутої за кордоном.
- Слідкуйте за новими схемами. Сьогодні шахраї рідко обіцяють «виграш у лотерею». Значно частіше вони маскуються під банки, «Нову пошту», «Укрпошту», Кіберполіцію, державні сервіси (включно з «Дією»), операторів зв'язку, роботодавців, родичів і колег.
- Звертайте увагу на сигнали підробки. Знеособлене звертання, граматичні помилки, скорочені посилання (bit.ly, cutt.ly тощо), дивні символи в адресі (наприклад, «roz3tka.ua» замість «rozetka.ua»), невідповідність відправника тексту повідомлення — усе це маркери фішингу. Ніколи не переходьте за посиланнями з SMS або месенджера: якщо сумніваєтеся, відкрийте офіційний застосунок банку чи сервісу самостійно або зателефонуйте на номер зі зворотного боку картки.
- «Терміново» — майже завжди підозріло. Шахраї свідомо створюють паніку: «картку заблоковано», «посилку повернуть», «рідний у лікарні та потрібні гроші». Саме цей емоційний тиск штовхає жертву до необдуманих дій. Зупиніться, передзвоніть родичу за відомим вам номером, зв'яжіться з банком через офіційний канал.
- Увімкніть двофакторну автентифікацію — але не через SMS. SMS-коди залишаються одним із найслабших способів підтвердження, особливо з огляду на SIM-свопінг. Де можливо, використовуйте застосунки-автентифікатори або ключі доступу (passkeys).
- Фіксуйте інциденти. Про підозрілі повідомлення варто повідомляти Кіберполіцію через cyberpolice.gov.ua або за номером 102. Це допомагає відстежувати схеми та блокувати інфраструктуру.

Окрема загроза: SIM-свопінг

Разом із SIM-фермами варто тримати у полі зору й іншу атаку на мобільний зв'язок — так званий SIM-свопінг, або підміну SIM-картки. У цій схемі шахрай не орендує номери, а переводить ваш номер під свій контроль: видає себе за абонента перед оператором і добивається переоформлення SIM-картки на нову «болванку». Отримавши контроль над номером, він має коротке вікно, аби перехопити SMS із кодами двофакторної автентифікації й зайти у ваш банк, месенджер чи поштову скриньку.

Перший сигнал такої атаки — раптове зникнення мобільного зв'язку: дзвінки й SMS перестають надходити без очевидних причин. У такій ситуації діяти потрібно негайно: зв'язатися з оператором з іншого номера, заблокувати SIM-картку, повідомити банк і змінити паролі до критичних сервісів. Для захисту від SIM-свопінгу варто встановити у свого оператора додаткове кодове слово для операцій із номером, увімкнути послугу заборони дистанційної заміни SIM-картки (де вона доступна), а також переходити з SMS-автентифікації на застосунки-автентифікатори та ключі доступу (passkeys).

Підсумок

SIM-ферми перетворили шахрайські SMS і дзвінки з разових махінацій на промисловість з готовими «коробковими» рішеннями для зловмисників. Окремі національні заборони та ліквідації мереж допомагають знижувати тиск, але не усувають загрозу повністю — тим паче поки значна частина інфраструктури розміщена у юрисдикціях, які не співпрацюють із західними правоохоронцями, і просувається серед російськомовної аудиторії. У цих умовах головним рубежем оборони залишається сам користувач: здорова недовіра до будь-якого «терміново», звичка перевіряти інформацію офіційними каналами та коректне налаштування автентифікації роблять атаки через SIM-ферми економічно невигідними для шахраїв.

Теги: США | SIM-ферма | криптоферма | Криптовалюта | Infrawatch | Беларусь | Білорусь | ProxySmart | Мошенничество | Шахрайство | кол-центр

Марія Войтенко
ОГЛЯДАЧ НОВИН

10 травня 2026 г., 22:28 Переглядів: 1769 Коментарі: 0

Роздрукувати Надіслати товаришу

Коментарі:

comments powered by Disqus