Доступ до облікового запису та підзвітність — Досьє Steam

Джерело: https://phishdestroy.io/steam_dossier/uk/investigation_part2
CC0 1.0 Universal · 2026-09-30

ДОСЬЄ «STEAM» / II

Ваш обліковий запис.Їхній доступ.*Хто відповідає?*

Автоматизація державних послуг. Аутсорсингова підтримка. А люди змушені розраховуватися за це.

Слідкуйте за станом інфраструктури, повідомленнями про збитки та документами, на яких ґрунтуються ці заяви.

Простежте інфраструктуру ↘
ДОДАТОК 01 / МОНІТОРИНГ РИНКУ «ЖИВИХ ТІНЕЙ»**550,000+**
Steam облікових записів, які активно виставлені на продаж на FSB Market (анонімізована назва; оригінальну назву тут не вказано)
саме в цю мить

550,000+ НАЯВНІСТЬ У РЕАЛЬНОМУ ЧАСІ · 231,829 В ІСТОРИЧНОМУ КОРПУСІ, ЗІБРАНОМУ ШЛЯХОМ СКРЕЙПІНГУ (198,320 ЛОГИ STEALER)
Головний підпільний центр обміну викраденими Steam-рахунками, `FSB Market` (інші пов’язані назви не вказано) здійснює аутентифікацію як покупців, так і продавців за допомогою офіційного OpenID Valve Steam (`openid.realm = https://FSB Market`). У будь-яку хвилину понад півмільйона вкрадених та зламаних облікових записів (журнали зломщиків із RedLine/Lumma, дані, отримані в результаті фішингу, атаки методом «credential stuffing») активно виставляються на продаж за копійки ($0.50–$2.00). Ні той, ні інший `FSB Market` ані `пов’язаний форум` блокується фільтром посилань Valve. Це промисловий резервуар, що постачає 63.06% платних акаунтів-ботів, які Valve блокує, не надаючи допомоги потерпілому.

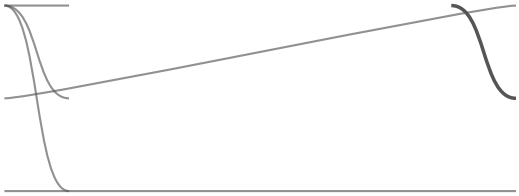
Live Intel: Моніторинг тіньового ринку (понад 550 тис. користувачів у режимі реального часу) ↗ · Відкрити запис про захоплення ↗ · Відкрити трасування фільтра посилань ↗Понад 550 тис. у прямому ефірі

01 / ЕКОСИСТЕМА З АВТОРАМИ

Автоматизація має*документальний ланцюжок.*

Названі проєкти. Опубліковані можливості. Відстежте інструмент за його документацією, а потім проаналізуйте зібрані взаємозв’язки розробників.

252ЗБІРНИКИ МАТЕРІАЛІВ
3,320ПРОФІЛІ НА GITHUB
4,214ПРОФІЛЬ — ПАРИ РЕПОЗИТОРІВ
Valve інфраструктура Громадські бібліотеки Додатки багаторазового використання



Лінії позначають задокументовані інтеграції або залежності. Виберіть вузол, щоб переглянути відповідні дані.

Автоматизація роботи з декількома обліковими записами / JustArchiNET

ArchiSteamFarm

Проєкт відкрито рекламує можливість одночасного фарму карт на різних облікових записах Steam. У файлі проєкту вказано залежність від SteamKit2.

Ознайомтеся з документацією самого проєкту ↗
SteamKit → ArchiSteamFarm
заявлена залежність ↗

ЗБІРКА ВІДНОСИН

40 мітки авторів · **40** етикетки «Forker»

Нижче наведено приклад від автора. Ці позначки описують зв’язок із репозиторієм, а не трудові відносини чи затвердження.

@JustArchi @renovate[бот] @JustArchi-ArchiBot @dependabot-preview[bot] (unavailable) @renovate-bot @actions-user @dependabot-support @Abrynos

Що показує графік розробника
На графіку відображено опубліковані дані про взаємозв’язки між авторами та розробниками, які створювали форки, у рамках зазначених проєктів та профілів GitHub. Це публічні дані — форки репозиторіїв, списки внесків, зв’язки між профілями. Питання полягає в тому, на що саме вимагає відповіді Valve на основі документальних доказів щодо опублікованих можливостей та взаємозв’язків розробників, а не в тому, що було вигадано в ході цього розслідування. Хеші вихідного коду зберігаються в походження карти.

Ознайомтеся з усією мережею ↗ Джерельні дані репозиторію ↓

02 / РІЗНІ ПОВНОВАЖЕННЯ. РІЗНІ ПОВНОВАЖЕННЯ.

Яка клавіша*Про що саме йдеться?*

Для гри гравцеві не потрібно надавати особистий ключ веб-API. Саме в цьому полягає головна відмінність, що лежить в основі даного розслідування.

01 / ОБЛІКОВИЙ ЗАПИС КОРИСТУВАЧА

Особистий ключ Web API

`steamcommunity.com/dev/apikey`

Видається з облікового запису користувача для дозволених викликів API. Створення ключів, їхня видимість, скасування та виявлення зловживань — це питання безпеки облікового запису.

02 / БЕКЕНД ІГРИ

Ключ Web API видавця

Партнери Steamworks використовують облікові дані видавця для виконання підтримуваних операцій на серверній стороні, зокрема для надання послуг, пов’язаних з іграми. Особистий ключ гравця є окремим обліковим елементом.

03 / ІДЕНТИФІКАЦІЯ ТА СЕСІЯ

OpenID / токени сеансу

OpenID підтверджує особу на веб-сайті. Сесійний або токен оновлення Steam має інше призначення. Ці механізми не слід подавати як один взаємозамінний «ключ API».

Valve містить ключі Web API як для користувачів, так і для видавців. Отже, Web API в цілому не є окремим від Steamworks. Документація щодо ключів API ↗ архів 2026-09-15 ↗ · Аутентифікація під час ігрової сесії ↗ архів 2026-08-29 ↗

СКЛАДЕНО АВТОРОМ ІНСТРУМЕНТУ / БЕРЕЗЕНЬ 2024 РОКУ

Для автоматизації можна використовувати не лише ключ API.

У вікі-сторінці «Trade Offer Manager» описано використання токена доступу сесії для окремих частин веб-API у випадках, коли окремого ключа API немає. Там також зазначено, що з кінця 2023 року для створення ключа потрібно підтвердження з мобільного пристрою. Розробник зазначає, що таке використання токена не підтримується версією Valve; це застаріла інформація з документації, а не результат реального тесту на обхід обмежень.

Ознайомтеся з поясненням відповідального за підтримку ↗ архів 2026-09-24 ↗

ЛЮДСЬКА СТОРОНА / ІЛЮСТРАТИВНИЙ ПРИКЛАД ФІШИНГУ

Все ще граю.*Вже викрито.*

Повідомлення від друга. Прохання проголосувати. Сторінка з подякою. Для гравця завдання виконано. Але зламаний сеанс може тривати й після цього моменту.

НА ЕКРАНІ ПЛЕЄРА

F
Розповідь друга
«Чи можете ви проголосувати за нашу команду?»

Запит надходить через чат Steam від знайомого акаунта. У цьому випадку пов’язана сторінка відкривається в браузері клієнта.

ПОЗА ПОЛЕМ ЗОРУ

Довіра виникає ще до появи веб-сайту.

Зламаний акаунт друга може додати довіри до фішингового посилання. Інтерфейс Steam, що оточує посилання, не підтверджує достовірність веб-сайту, на який веде посилання.

ЗНАЙОМИЙ ВІДПРАВНИК / ЗОВНІШНЄ МІСЦЕ ПРИЗНАЧЕННЯ

Безпека облікового запису — це питання, яке слід вирішити перед продажем будь-якого товару.
Гравець не мав наміру створювати облікові дані для автоматизації або делегувати контроль. Повернення до гри не є доказом того, що обліковий запис є безпечним. Valve зберігає журнали сеансів, записи про створення API-ключів та дані про кореляцію пристроїв. А жертва — ні. Саме ця асиметрія і є проблемою відповідальності.

Доступ до сеансів та типи облікових даних
Ключ API та сесія входу — це окремі облікові дані з різними можливостями. Скасування ключа не призводить до припинення активної сесії. У власній документації Valve описано обидва ці елементи; Valve зберігає журнали, які покажуть, які саме облікові дані були активними на момент будь-якої спірної дії. Вимога полягає у розкритті саме цього запису — а не у висновках, вигаданих у ході розслідування. Документація розробника щодо роботи з токенами ↗ архів 2026-09-24 ↗ · Valve ключова документація ↗ архів 2026-09-15 ↗

03 / ОФІЦІЙНИЙ РИНОК МАЄ СВОЮ ГРАНІЦЮ

Цей предмет може бути рідкісним.*Обмеження залишається в силі.*

Ціну, що перевищує встановлений ліміт, неможливо реалізувати шляхом розміщення одного оголошення на «Community Market» за цією повною ціною.

Орієнтовна ціна продажу$5,000Змінити ціну, за яку виставлено товар
$100 $20,000
Ілюстрація опублікованого ліміту, а не оцінка або рекомендація щодо торгівлі.

ЛІМІТ РОЗМІЩЕННЯ ≈ **$1,800**
КРИШКА ГАМАНЦЯ ≈ **$2,000**
Вище встановленого ліміту розміщення.

Кошти з гаманця не можна вивести на банківський рахунок. Ці обмеження породжують попит, який задовольняють сторонні ринки скінів: попит, що виникає внаслідок обмежень на розміщення оголошень та лімітів гаманців, тоді як власні правила Valve забороняють комерційним операторам його задовольняти.

Ринкові обмеження Steam ↗ архів 2026-09-21 ↗

04 / В МЕЖАХ ЗОНИ ПІДТРИМКИ

Нам довірено дані.*Відповідає за доступ.*

Політика конфіденційності компанії Valve прямо передбачає передачу персональних даних стороннім постачальникам послуг технічної підтримки, якщо це необхідно для надання такої підтримки.

ГРАВЕЦЬ **Рахунок та підтверджуючі документи**
→
КЛАПАН **Процес відновлення**
→
НАДАВЕЦЬ ПОСЛУГ **Делегований доступ**
Політика конфіденційності, §5.2 ↗ · Згідно з власною політикою компанії Valve, стороннім особам надається доступ для технічної підтримки. Залишаються відкритими такі питання: які саме дозволи були надані, які існують журнали аудиту та що сталося, коли, як стверджується, цим доступом було зловжито.

2015

Шкала була загальнодоступною

Valve визнала факт масового викрадення облікових записів та описала заходи захисту.

Valve публікація ↗ архів 2026-08-09 ↗

2015

Valve передала цю роботу на аутсорсинг — і про це заявила

Valve має невелику внутрішню команду керівників служби підтримки Steam і заявила про це *«залучив кілька різних компаній»* для забезпечення технічної підтримки (Erik Johnson, Valve, для Kotaku); пункт 5.2 її політики конфіденційності надає цим третім сторонам право доступу до даних користувачів. **Який підрядник має доступ до відновлення облікового запису, Valve ніколи не розкривав** — У дискусіях у спільноті згадуються такі постачальники, як Concentrix, але жоден із них не Valve-підтверджений. Відділ, робота якого була передана на аутсорсинг, існував ще за кілька років до будь-якого з наведених нижче визнань.

Kotaku: Valve щодо підтримки ↗ архівувати 2025-07-11 ↗

2023

Перше зарахування

Команда Valve з CS:GO письмово бере на себе відповідальність за злом облікового запису, що стався через її власну процедуру звернення за допомогою, та скасовує обміни.

Відкрити справу щодо аутсорсингу ↓

2025

Друге зарахування

Через 33 місяці служба підтримки Steam повідомляє, що технічний спеціаліст «не дотримався нашої процедури, внаслідок чого ваш обліковий запис було відновлено на ім’я іншої особи». Той самий канал. Той самий результат.

Dexerto, 14 листопада 2025 р. ↗

МАТЕРІАЛИ СПРАВИ / HFB ТА ЗВИНУВАЧЕННЯ У ВИКОРИСТАННІ АУТСОРСИНГУ

Шлях до входу — це сама підтримка Steam. *Valve зазначив це в письмовій формі.*

У відповіді служби підтримки, опублікованій на сайті Dexerto, команда Valve з CS:GO бере на себе відповідальність за злам облікового запису **у процесі подання запиту на допомогу** — через власний канал, а не через фішингову сторінку чи користувача. Активи було відновлено, а операції скасовано, що, як зазначає Valve, є засобом захисту, якого, за його словами, у інших жертв немає. За повідомленнями, запаси HFB становили **$2,000,000+** в той день і **$3,000,000+** у подальшому; **Qkss програв $1,000,000+ таким самим чином і нічого не отримав**.

ВІДПОВІДЬ СЛУЖБИ ПІДТРИМКИ / Опубліковано DEXERTO · 21 лютого 2023 року

> «зламано через запит на технічну підтримку, відповідальність за що бере на себе команда CS:GO»

Ознайомтеся зі звітом та наведеним повідомленням ↗ архів 2025-08-18 ↗

01 / ЯКИЙ КЛАПАН ВСТАНОВЛЕНО

Саме власний канал підтримки став тим самим шляхом

У відповіді йдеться про зламаний обліковий запис та скасування пов’язаних з ним операцій. Valve скасував їх — отже, ці операції можна було скасувати. Оригінальний автентифікований квиток у цій колекції відсутній.

02 / ЧОГО НЕ ВДАЛОСЯ ВИРІШИТИ ЗВІЛЬНЕННЯМИ

Ці самі двері знову відчинилися в листопаді 2025 року

Підрядник звільнив весь свій персонал служби підтримки Steam — про це повідомило видання Mzkshow з посиланням на Dexerto; це не було офіційним повідомленням Valve від компанії. Через тридцять три місяці Steam Support написав іншому колектору, що «технічний спеціаліст служби підтримки, який обробляв запит на допомогу, не дотримався нашої процедури, що призвело до відновлення вашого облікового запису на ім’я іншої особи». Це цитата з повідомлення Valve щодо того самого каналу.

Друга госпіталізація, 14 листопада 2025 року ↗
03 / ЩО ТАКЕ «ВІДКРИТЕ»

Valve ніколи не називав підрядника

Ці джерела не вказують ані підрядника, ані місцезнаходження. Це не прогалина у звітності — це інформація, яку Valve не оприлюднила щодо того, хто мав доступ до облікових записів користувачів.

Сучасний опис цієї справи ↗
Три питання, на які Valve не відповів: хто міг скасувати відновлення облікового запису, що виявив аудит доступу та що змінилося після цього.

Пізніші звинувачення, що містяться в збереженому архіві доказів
Два дописи на Reddit за 2024 рік містять інформацію про подальші розслідування Mzkshow — випадок скасування блокування VAC у липні 2024 року та випадок з інвентаризацією $13,000 у грудні 2024 року. Це окремі інциденти, про які повідомляється окремо. Питання відповідальності в кожному з них однакове: хто мав права на обхід обмежень, що виявив аудит і що змінилося.

14 липня 2024 року · повідомлено про одужання / VAC-випадок заборони ↗ 2 грудня 2024 року · зареєстровано $13,000 випадків з запасами ↗ архів 2025-08-05 ↗ Два збережені пости, рядки джерел та хеші ↓

05 / СЛІДКУЙ ЗА ВТРАТОЮ

Будь-яка сума*потрібен футляр.*

Десять випадків, червень 2022 року — березень 2026 року. Кожна цифра відповідає даним, опублікованим у зазначеному джерелі — **$6,300,000**, **$2,000,000+**, **$1,000,000+**, **≈$320,000**, **≈$300,000**, і аж до 288 євро. Valve зберігає журнал транзакцій, запис сеансу та аудиторський слід підтримки для кожної з них, але не надав жодного з них.

КАНАЛ ПІДТРИМКИ 21 червень 2022
$2,000,000+

HFB — the largest inventory in the game

ЗВІТ ПРО ОЦІНКУ ВАРТОСТІ ЗАПАСІВ · ЗБІЛЬШЕННЯ ДО $3M+ У ЛЮТОМУ 2023 ПІДСУМКИ

Сім сувенірних «Dragon Lores» та «Blue Gem Karambit» з номером #1; лише цей ніж коштує приблизно $1.26. Акаунт не використовувався три роки, автентифікатор залишався увімкненим; електронну адресу та пароль було змінено через процедуру відновлення, надану службою підтримки. Компанія «Valve» скасувала транзакції — та письмово підтвердила свою відповідальність. До скасування транзакції, за повідомленнями, вже було знято понад $200,000через market.csgo.com, який здійснює розрахунки готівкою та криптовалютою. Скасування повертає скін, а не гроші, які хтось уже переказав на рахунок. Відміна угоди також призвела до збою: покупець сховав свій «Souvenir Dragon Lore» у внутрішньоігровому сховищі, скрипт не зміг заглянути всередину цього контейнера, а Valve продублював предмет вартістю $130,000 під час скасування крадіжки — це було виявлено за ідентифікаторами предметів та повідомленнями спільноти, а в липні 2022, покупець отримав відшкодування від BUFF, а не від Valve.

Dexerto, день крадіжки ↗

ГАМАНЕЦЬ ТА ПОКУПКИ 07 ЛИПНЯ 2022
>$500

44 disputed Market purchases

ЗАДЕКЛАРОВАНІ ВИТРАТИ З ГАМАНЦЯ · USD

Користувач повідомляє про несанкціоновані покупки недорогих предметів у грі Dota 2 та незадовільну реакцію служби підтримки.

Ознайомтеся зі скаргою та скріншотами за посиланням ↗

ВТРУЧАННЯ У РОБОТУ ПЛАТФОРМИ 14 2022 серпня
$6,300,000

CS.Money — 19,000+ скіни з ботів

ОЦІНКА ВАРТОСТІ · ПЕРША ОЦІНКА $1.6M

Зловмисники викрали файли мобільних аутентифікаторів торгових ботів торговельної платформи та очистили їх, переказавши частину викрадених коштів відомим трейдерам, щоб заплутати сліди. Дослідники з спільноти за лічені години склали карту акаунтів зловмисників 55. Valve нічого не скасував — сторонній сайт знаходиться поза межами Steam, повідомив той самий Steam, чиї запаси, торгова платформа API та система обліку стали об’єктом крадіжки від початку до кінця.

Прочитайте сучасний опис подій ↗

КАНАЛ ПІДТРИМКИ Publikація: 21 ФЕВРАЛЬ 2023
$1,000,000+

Qkss — ті самі двері, той самий актор, протилежна відповідь

ЗАДЕКЛАРОВАНА ВАРТІСТЬ ЗАПАСІВ

Це відбулося так само, як і у випадку з HFB: тим самим актором, через той самий запит до служби підтримки. Проблема з HFB була повністю вирішена за вісім місяців до цього. А з Qkss — ні. У опублікованих даних немає нічого, що відрізняло б ці два випадки, окрім чисельності аудиторії.

Dexerto про розслідування Mzkshow ↗

КАНАЛ ПІДТРИМКИ ОПУБЛІКОВАНО 2023
≈ $320,000

Сама інсайдерська торгівля — один рік такої діяльності

РЕЗУЛЬТАТИ ДІЯЛЬНОСТІ ЗА ПРИБЛИЗНО ОДИН РІК · ЦЕ НЕ ОЦІНКА ВАРТОСТІ ЗАПАСІВ

Служба підтримки отримала доступ до історії облікового запису за останні 15 років: перший CD-ключ, перший електронний лист, перша картка — саме ті докази, яких вимагає процедура відновлення. Той, хто володіє базою даних, завжди виграє суперечку з тим, хто володіє обліковим записом. Один вкрадений M4A4 Howl з голограмами iBUYPOWER та Titan Katowice 2014 був проданий за $35,000 і в підсумку опинився у b1t з команди NAVI, який не мав можливості про це дізнатися. Відповіддю підрядника стало звільнення всіх співробітників, які працювали в службі підтримки Steam.

Escorenews про це ж розслідування ↗

ГАМАНЕЦЬ ТА ПОКУПКИ 09 DEC 2023
€288

Втрата гаманця попри двоступеневий захист

TRUSTPILOT · ІНДЕКС ДЖЕРЕЛ 16

Рецензент повідомляє про злом облікового запису та відмову надати допомогу щодо витрат у Market. У експортованому файлі немає індивідуальної URL-адреси відгуку.

Перевірити походження джерела ↗

ВІДНОВЛЕННЯ ОБЛІКОВОГО ЗАПИСУ 02 DEC 2024
$13,000

«Матвій» — через два роки після звільнень

ОЦІНКА ЗАПАСІВ АВТОРА

Відновлення доступу було надано особі, яка надала дані облікового запису, які сам власник не зміг підтвердити. Той самий шлях, той самий результат — після того, як підрядник ліквідував свою службу підтримки Steam.

Ознайомтеся зі збереженим звинуваченням ↗

ВІДНОВЛЕННЯ ОБЛІКОВОГО ЗАПИСУ 09 ТРАВЕНЬ 2025
≈ $10,000

Відновлення за допомогою чужого квитка

ЗАЯВЛЕНА ВТРАТА ТОВАРУ · Долари США

Користувач із Квебеку стверджує, що служба підтримки скинула пароль і скасувала захист облікового запису на прохання іншої особи.

Прочитайте скаргу, написану від першої особи ↗

КАНАЛ ПІДТРИМКИ 13 112025
≈ $300,000

Hawkeye337 — і друге письмове зізнання від «Valve»

ПОВНА КОЛЕКЦІЯ HOLO «2014» З КАТОВИЦЬ

Зловмисник вимагав 1 біткойна і почав переносити колекцію на Negevs, щоб знищити її. Steam Відповідь служби підтримки: «Технічний спеціаліст, який обробляв запит на допомогу, не дотримався нашої процедури, що призвело до відновлення вашого

облікового запису на ім’я іншої особи». Через тридцять три місяці після першого визнання — та сама ситуація. Акаунт було відновлено за кілька годин після того, як ця тема стала популярною на X. У Qkss не було такої аудиторії.

Dexerto, 14 Nov 2025 ↗

ГАМАНЕЦЬ ТА ПОКУПКИ 29 MAR 2026
$50

Несанкціоноване поповнення рахунку та ігри, отримані в подарунок

TRUSTPILOT · ІНДЕКС ДЖЕРЕЛ 290

Рецензент заявляє про несанкціоновані витрати та відхилені запити на повернення коштів. У файлі експорту відсутня URL-адреса окремого відгуку.

Перевірити походження джерела ↗

Джерела та суми залишаються такими, як зазначено в кожному джерелі. Valve зберігає журнали транзакцій, записи сеансів та аудиторський слід підтримки для кожного з цих випадків. Надайте їх. Збережений допис на Reddit не вирішує питання — вирішують власні записи Valve.

КОЛЕКЦІЯ / ПІСЛЯ ПЕРЕВІРКИ

231,829 облікових записів на продаж. *Valve містить журнали для кожного з них.*

354 → 201

Відгуки на Trustpilot

Видалено 153 дублікати рядків. URL-адреси окремих оглядів не були збережені під час експорту.

231,829

Steam перелік облікових записів

33,509 класифікується як «самостійно зареєстрований»; 198,320 під маркою «колекціонер-крадій». Оголошення не є завершеними угодами.

Аудит колекції ↓ Пошук у архіві вихідного коду ↗