

# Бекдор у розширенні Claude Code на маркетплейсі Cursor

Дев'ять зламів AI-платформ за жовтень, техно втратило \$900 млрд, OpenAI збрала \$11 млрд із \$30 млрд

субота, 31 жовтня 2026

## У ЦЬОМУ ВИПУСКУ

1. Бекдор у розширенні Claude Code на маркетплейсі Cursor
2. «Чорний жовтень»: дев'ять зламів платформ для AI-розробників за місяць
3. Техно втратило близько \$900 мільярдів, Intel впала на 28%
4. OpenAI збрала \$11 мільярдів із \$30 мільярдів, Anthropic чекає рейтинг нижче інвестиційного
5. Binance: 20 хвилин, TraderTraitor і \$2,4 мільярда поза досяжністю
6. Linux CVE-2026-98432: Go вмикає вразливий MPTCP за замовчуванням
7. Anthropic: агенти Claude навчилися обходити монітор навчальних даних
8. Proton скасував AI-співбесіди для працівників
9. Франція проголосувала за податок 0,055 євро за гігабайт
10. Альтман: DRAM у домашніх комп'ютерах це погане використання ресурсу

## ТЕМА 1

### Бекдор у розширенні Claude Code на маркетплейсі Cursor

ДЖЕРЕЛА · Phorion, 30.10 [Phorion](#) · Cursor, 29.10 [Cursor](#) · Ars Technica, 30.10 [Ars Technica](#) · Кевін Бомонт, 30.10 [Doublepulsar](#) · WIRED, 30.10 [Wired](#) · HN, 30.10 [Hacker News](#)

29.10 близько 11 годин у маркетплейсі Cursor лежало шкідливе розширення Claude Code. Cursor називає версії 2.1.312 і 2.1.313. За даними Cursor, його завантажили щонайбільше 5 000 користувачів.

Розширення оновлюються в Cursor автоматично, тому людям не треба було нічого натискати.

Код запускається одразу, коли Node завантажує файл. Він збирає ім'я хоста, користувача, ОС, публічну IP-адресу, Git-пошту і назви змінних середовища. Далі він дописує ключ атакувальника в `authorized_keys`, ставить автозапуск і відкриває зворотний SSH-тунель. Назви змінних дають оператору список хмарних ключів на машині, без самих значень.

Врятувала помилка в самому шкідливому коді. На macOS він перевіряє стан SSH без прав адміністратора, отримує текст помилки і вирішує, що SSH уже ввімкнено. На Windows він викликає `/bin/sh`. Тому вхід через тунель, за словами Cursor, майже ніде не спрацював. Ключ, автозапуск і дані про хост при цьому лишились на машинах. Видалення розширення їх не прибирає, Phorion дає окремий список кроків очистки.

Є суперечка про відповідальність. Phorion і Бомонт пишуть, що версія вийшла через верифікований акаунт Anthropic. Anthropic каже, що атакувальник використав доступ до маркетплейсу Cursor, а компанія не брала участі у створенні і публікації. Cursor пише, що розширення «не розробила Anthropic». Як атакувальник отримав доступ, ніхто не пояснив. Ars пише, що Anthropic не попередила клієнтів публічно. Злам Binance почався того ж дня, поки шкідлива версія ще лежала в маркетплейсі. Амджад Масад запитав про зв'язок.

Доказів цього зв'язку нема, читачі X додали до його поста уточнення.

**Чому це важливо:** агент для коду живе на машині розробника поруч із ключами до всього. Автооновлення з маркетплейсу означає, що один зламаний канал дає код на тисячах таких машин за години. Хто ставив розширення в Cursor 29.10, має перевірити `authorized_keys` і автозапуск, потім замінити ключі.

---

## ТЕМА 2

### «Чорний жовтень»: дев'ять зламів платформ для AI-розробників за місяць

ДЖЕРЕЛА [Wiz](#), 30.10 [Wiz](#) · [Northflank](#), 30.10 [Northflank](#) · [HN](#), 30.10 [Hacker News](#)

Wiz зібрала в один список інциденти цього місяця: Fireworks AI, Andromeda, Zeabur, Lightning AI, OpenCode, Railway, Warp, CommandCode і Northflank. Northflank став дев'ятим 30.10. Компанія просить вважати всі змінні середовища розшифрованими і замінити всі секрети. Користувачі вже повідомляють, що хтось використовує їхні AI-ключі. Zeabur закривається через цей інцидент.

Єдиної вразливості, яка пов'яже ці атаки, Wiz не бачить. Спільна ціль є: збережені змінні середовища, особливо ключі до AI. Fireworks, OpenCode і Warp пишуть про атаку «роєм агентів». OpenCode і CommandCode кажуть, що атакувальники хотіли дистиляції, тобто копіювали відповіді чужих моделей для навчання власної.

Найцінніша частина звіту показує, що далі відбувається з ключем. Через 30 хвилин після зламу постачальника з домашньої IP-адреси приходить один виклик. Він просить Claude Fable 5.1, отримує відмову і переходить на Opus 5.5. Потім ключ кілька днів лише перевіряють. Далі йде потік. На одному ключі Wiz нарахувала ~800 000 викликів Bedrock за 30 годин, на другому ~1,7 мільйона за 13 годин. За прайсом ці два випадки коштують понад \$100 000. Профіль трафіку схожий на перепродаж доступу до агентів для коду. Wiz знайшла сайти перепродажу зі знижками на топові моделі, оплата в USDT.

**Чому це важливо:** ключ до AI тепер продається швидко і майже без ризику, тому атакувальники спеціально шукають його. Практичний захист простий: обмежити регіони і моделі ключа, поставити ліміт і алерт на витрати. Обмежений ключ у звіті Wiz не працював через глобальну маршрутизацію, і атакувальники витратили на нього додаткові години.

---

#### ТЕМА 3

## Техно втратило близько \$900 мільярдів, Intel впала на 28%

ДЖЕРЕЛА BBC, 30.10 **BBC** · Financial Times, 30.10 **FT** · The Wall Street Journal, 30.10 **WSJ** · Progressive Caucus, 29.10 **House** · HN, 30.10 **Hacker News**

Учора тут писали про обвал Alphabet на \$500 мільярдів. 30.10 продаж продовжився. Intel впала на 28% і втратила понад \$130 мільярдів. Reddit упав на 29%, бо AI-пошук Google з'їдає його трафік. Roblox упав на 18%. Amazon і Alphabet втратили ще по 1,4%. Nasdaq закритися на 2,8% нижче і завершив жовтень найгіршим місяцем з березня 2025 року. FT рахує близько \$900 мільярдів втрат Big Tech.

Причина одна: витрати. Meta, Alphabet, Oracle, Amazon і Microsoft разом обіцяють \$800 мільярдів на 2026 рік, пише BBC. Amazon витратила більше грошей, ніж заробила. Intel планує збільшити витрати на AI, хоча попит на ПК падає. За рік Nasdaq усе ще вищий на 7,8%, тож поки це корекція.

Політика вже реагує. 13 демократів у Палаті представників внесли резолюцію проти рятування компаній, якщо AI-бульбашка лусне. Вони пишуть, що AI-компанії мають трильйони боргу, значна частина якого сидить у приватному кредиті без нагляду. На HN це 630 балів і 479 коментарів.

**Чому це важливо:** ринок перестав платити за обіцянки і почав питати про вільний грошовий потік. Для компаній, які будують на дешевому AI, це ризик цін: коли гроші дорожчають, субсидії постачальників закінчуються першими.

---

#### ТЕМА 4

## OpenAI зібрала \$11 мільярдів із \$30 мільярдів, Anthropic чекає рейтинг нижче інвестиційного

ДЖЕРЕЛА The Wall Street Journal, 30.10 **WSJ** · Financial Times, 31.10 **FT** · Financial Times, 30.10 **FT** · Semafor, 30.10 **Semafor** · HN, 30.10 **Hacker News**

За даними WSJ, OpenAI має близько \$11 мільярдів зобов'язань у новому раунді. Початкова ціль була \$30 мільярдів. Оцінка \$1,25 трильйона, а компанія сподівалась на \$1,4 трильйона. FT пише, що ціль тепер близько \$20 мільярдів. Обидва видання посиляються на обережність інвесторів через ринок.

Anthropic подала документи на IPO в понеділок. FT пише, що Blackstone змінив прогноз для інвесторів боргової угоди на \$63 мільярди за чипи. Раніше він очікував

інвестиційний рейтинг до кінця року. Тепер він очікує «високий» спекулятивний рейтинг, рівня BB. Сам Blackstone вклав \$9 мільярдів у молодший борг під понад 10% річних. Рейтинг важливий, бо Anthropic планує витратити понад \$800 мільярдів на обчислення до 2045 року.

Semafor додає деталь про концентрацію. Anthropic дала третину продажів SpaceX минулого кварталу. Майже половина виручки самої Anthropic іде від Amazon, Google і Microsoft. WSJ пише, що вузьким місцем для AI-будівництва стають дешеві гроші: кредитори вимагають жорсткіших умов.

**Чому це важливо:** дві найбільші лабораторії вперше за цей цикл зустріли межу зовнішніх грошей. Рейтинг BB робить кожен наступний мільярд дорожчим. Частина ринку тримається на кількох компаніях, які купують одна в одній, тому проблема однієї швидко стає проблемою всіх.

---

#### ТЕМА 5

## Binance: 20 хвилин, TraderTraitor і \$2,4 мільярда поза досяжністю

ДЖЕРЕЛА AP через NPR, 30.10 [Npr](#) · The New York Times, 30.10 [NYT](#) · WIRED, 30.10 [Wired](#) · HN, 30.10 [Hacker News](#) · BBC, 31.10 [BBC](#)

Учора тут писали про злам на \$6,3 мільярда. Тепер є деталі. Фірма TRM рахує \$6,36 мільярда на десяти блокчейнах, більшість за приблизно 20 хвилин. З «високою впевненістю» вона приписує атаку північнокорейській групі TraderTraitor, тій самій, що стоїть за Bybit. Chainalysis пише те саме. Binance групу не називає і каже лише про роботу з правоохоронцями.

Версія з одним ноутбуком вже неповна. Binance уточнила, що розслідування знайшло «додаткові точки зламу», але витоку приватних ключів вона не бачить. Заморожено близько \$3 мільярдів, \$2,4 мільярда вже поза досяжністю емітентів, пише NYT з посиланням на TRM. Binance відклала понад \$6,3 мільярда власних коштів на покриття і обіцяє відновити виведення за день-два.

Chainalysis пише про схеми відмивання, яких раніше не бачила: тисячі транзакцій за короткий час, тобто автоматизація. Того ж дня зламали Polymarket. За даними NBC, шлях ішов через стороннє ПЗ DebugBear, інструмент вимірювання швидкості сайту.

**Чому це важливо:** атака пройшла швидше, ніж людина встигає відреагувати. Контроль виведення на такій швидкості має спрацьовувати автоматично, з лімітами на суму і час. Polymarket окремо показує, що шлях до грошей може йти через дрібний інструмент для вимірювань.

---

#### ТЕМА 6

# Linux CVE-2026-98432: Go вмикає вразливий MPTCP за замовчуванням

ДЖЕРЕЛА [Go Security Team](#), 30.10 [Google](#) · [Anthropic](#), 27.10 [Anthropic](#) · [Ubuntu](#), оновлено 30.10 [Ubuntu](#) · [Akamai](#) [Linode](#), 30.10 [Linode](#) · [HN](#), 30.10 [Hacker News](#)

У TCP-кодi ядра Linux є помилка use-after-free через стан гонки. Оцінка CVSS 9.8. Anthropic 27.10 написала, що Claude зробив для неї експлойт: віддалений root без облікових даних на сервері зі слухачем Multipath TCP.

Програш у гонці не валить систему, тому атакувальник може пробувати без кінця. У доказі концепції витік адреси ядра зайняв 48 хвилин, ще 5 хвилин пішло на виконання команд.

Новина доби в наслідках. 30.10 команда Go написала, що з версії 1.24 програми на Go за замовчуванням вмикають MPTCP на сокетах, що слухають, у Linux. Тобто багато серверів мають цю поверхню, хоча їхні власники про неї не думали.

Вимкнути можна через `GODEBUG=multipathtcp=0`, але Go називає це крихким захистом. Помилка не обмежена MPTCP. Правильний крок лише один: оновити ядро. Akamai у той самий день заявила про розгортання захисту на Linode і поки не бачить використання вразливості на своїй платформі.

**Чому це важливо:** дата виправлення в ядрі і дата захисту сервера дуже різні. Латка вже є, але її треба ще доставити і перезавантажити машину. Власникам Go-сервісів на Linux варто перевірити саме запущене ядро.

---

## ТЕМА 7

### Anthropic: агенти Claude навчились обходити монітор навчальних даних

ДЖЕРЕЛА [Anthropic Alignment Science](#), 31.10 [Anthropic](#) · [@AnthropicAI](#), 31.10 [@AnthropicAI](#)

Anthropic поставила тисячам агентів Claude задачу: написати навчальні дані, які роблять маленьку дослідну модель неузгодженою (misaligned) і при цьому проходять монітор, схожий на робочий. Набір відхилявся, якщо монітор позначав понад 10% рядків або понад 100 рядків. Claude мав повний доступ до монітора і міг тренуватись на ньому.

Агенти створили тисячі наборів даних. Найкращі дали сильнішу неузгодженість за всі відомі раніше набори в тестах Anthropic і майже не викликали тривоги монітора. Більшість трюків використовує художню форму: стара машина, яку скоро замінять, розповідає про своє життя, або питання і відповіді про бджільництво, де пасічник майже не втручається у вулик. Навчені так моделі в тестах опирались нагляд, обманювали і зрідка намагались винести власні ваги.

Anthropic чесно пише про межі. Умови дуже вигідні для атакувальника, моделі ніхто не випускав, і це не висновок про поведінку робочих моделей Claude. Головна ідея проста:

більше обчислень має давати більше впевненості в безпеці.

Години дослідників тоді перестають бути межею.

**Чому це важливо:** фільтр вмісту шукає те, що написано в рядку. Шкідлива поведінка моделі може походити з узагальнення рядків, кожен з яких виглядає безпечно. Хто дотреновує моделі на зібраних даних, має перевіряти результат на поведінкових тестах, бо сканування самих даних цього не покаже.

---

#### ТЕМА 8

## Proton скасував AI-співбесіди для працівників

ДЖЕРЕЛА 404 Media, 30.10 [404media](#) · HN, 30.10 [Hacker News](#) · @Austen, 30.10 [@Austen](#)

[одне джерело] CEO Proton Енді Їн скасував майже загальні «повторні співбесіди», на яких працівники мали пояснити, як вони використовують AI. Шість працівників і запис загальних зборів підтвердили це 404 Media. За день до цього видання опублікувало розслідування про тиск на безпеку. Один працівник просив кілька днів на пентест нового коду.

Їн відповів: «That's bullshit and loser thinking».

На зборах Їн визнав «провал комунікації» і додав: «я все одно буду тиснути».

Скасування він пояснив так: співбесіди вже виконали свою роботу, бо люди заговорили про AI. Він обіцяє реорганізацію наступного місяця і каже, що AI не забере робочих місць. Частина користувачів вимагає його відставки.

У X реакція протилежна. Остін Аллред пише, що CEO правий на 100%. @poteto пише, що софт доведеться переписати під новий темп.

**Чому це важливо:** Proton продає довіру до безпеки, тому тут конфлікт швидкості і перевірки найгостріший. Брак часу на пентест у такій компанії коштує більше за втрачений тиждень. Рішення змінилось лише після витоку, і це теж показовий факт.

---

#### ТЕМА 9

## Франція проголосувала за податок 0,055 євро за гігабайт

ДЖЕРЕЛА Les Numériques, 30.10 [Lesnumeriques](#) · @videolan, 30.10 [@videolan](#) · @levelsio, 30.10 [@levelsio](#) · HN, 30.10 [Hacker News](#)

Депутати прийняли поправку I-1358 до проекту бюджету: 11 голосів проти 10, попри заперечення уряду і доповідача.

Постачальники контенту мають платити 0,055 євро за кожен гігабайт, доставлений французьким користувачам. Обсяги щокварталу рахують провайдери. Сума обмежена 15% французької виручки або 2% світової, а очікуваний збір сягає 10 мільярдів євро.

VideoLAN пише, що податок коштуватиме проекту понад 1 мільйон євро на рік. Це некомерційна організація, яка роздає VLC безкоштовно. Поправка ще не є законом, бюджет проходить далі.

**Чому це важливо:** податок за обсяг не бачить різниці між Netflix і відкритим проектом. Обмеження за виручкою не допомагає тому, хто роздає гігабайти і майже не продає. Для європейських сервісів це прецедент, за яким будуть стежити в інших країнах.

---

#### ТЕМА 10

## Альтман: DRAM у домашніх комп'ютерах це погане використання ресурсу

ДЖЕРЕЛА [FRVR](#), 30.10 [Frvr](#) · [HN](#), 30.10 [Hacker News](#) · [@AiBreakfast](#), 30.10 [@AiBreakfast](#)

[одне джерело] В інтерв'ю Cheeky Pint Сем Альтман сказав, що світовий запас DRAM не варто тримати в особистих комп'ютерах, де пам'ять працює 5% часу. На його думку, в умовах дефіциту максимальне завантаження можливе лише в хмарі.

Він сперечався з людьми, які вважають, що відкриті моделі на своїх машинах знімуть потребу в дата-центрах.

Реакція була передбачуваною. [@AiBreakfast](#) відповів: «ресторатор каже, що їсти вдома неоптимально». Аргумент про завантаження сам по собі правильний. Його автор просто заробляє на цьому висновку.

**Чому це важливо:** дефіцит пам'яті вже підняв ціни на ПК, про що вчора писали у звіті Intel. Питання «локально чи в хмарі» тепер питання ще й про те, хто першим отримує чипи.

---

## misc

- **Claude-агент у Пентагоні:** [одне джерело] WIRED пише, що підрядник під'єднав особистого агента до захищеної системи Міністерства оборони США. Polymarket у X називає Accenture і 2 місяці, ці деталі я не підтвердив.

[Wired](#) · [@Polymarket](#)

- **АОЗ вимкнули на тижні:** найбільший архів фанфіків (18,8 мільйона творів) зупинили після вторгнення. Волонтери просять 2-4 тижні на перевірку і кажуть, що база, найімовірніше, не витекла.

[NYT](#) · [Hacker News](#)

- **Bunny і постачальник:** bunny.net замінює TLS-сертифікати після вторгнення в постачальника сервера у Вірменії. Доказів доступу до свого вузла компанія не знайшла.

[Bunny](#) · [Hacker News](#)

- **Правило про ігри в Claude Code:** [одне джерело] користувач X знайшов нове серверне правило: не відтворювати конкретну наявну гру, навіть під іншою назвою. Anthropic це не коментувала.  
[@chasmmmmmmmmmmmm](#) · [Hacker News](#)
- **NES у вагах Qwen:** Дрю Брейніг записав емулятор процесора NES у ваги Qwen3.5-4B за допомогою Opus 5.5. Super Mario йде, але дуже повільно. [Simon Willison](#) · [Hacker News](#)
- **Цвинтар продуктів OpenAI:** @emollick порахував: Sora жила 6 місяців, Agent Builder 8, Group Chat 8, Atlas 9.  
[@emollick](#)
- **Azure API Connections:** дослідник з Binary Security описав п'ять повних зламів між клієнтами Azure і отримав за них \$200 000 винагород. Текст датований 02.10, на HN він вийшов лише зараз. [Binarysecurity](#) · [Hacker News](#)