AI-ДАЙДЖЕСТ

Claude Code лишає паролі з команд на GitHub

Apiiro знайшла 1 122 публічні файли Claude Code зі справжніми паролями і ключами з команд.

неділя, 8 листопада 2026

У ЦЬОМУ ВИПУСКУ

1. Claude Code записує паролі з команд у файл, і цей файл потрапляє на GitHub
2. MaxxBench: малі зміни вимог розводять «рівні» моделі на 23 пункти
3. Microsoft закрила групу AI Frontiers, її засновник пішов
4. На кожному Mac працює граф знань про власника і його родину
5. Справа Хуанга: FT пише про пам'ятку розвідки, сенатор обіцяє розслідування
6. Будівництво дата-центрів упирається в електрику і воду
7. Практики знімають зайві запобіжники: моделі вже кращі за них
8. Discord на Rust: клієнт стартує одразу і бере на 70% менше пам'яті
9. Unitree: роботів збирають руками, і це економічно правильно
10. Ставки на Polymarket за годину до опитування NYT

ТЕМА 1

Claude Code записує паролі з команд у файл, і цей файл потрапляє на GitHub

ДЖЕРЕЛА Apiiro, 05.11 Apiiro · HN, 07.11 Hacker News

Механіка проста. Агент пропонує команду, наприклад запит до бази, і в команді стоїть пароль з конфігу. Користувач натискає «Yes, and don't ask again». Claude Code зберігає цю команду дослівно, разом з паролем, як правило дозволу у `.claude/settings.local.json` у теці проєкту.

Claude Code додає цей файл у глобальний gitignore розробника, але лише коли створює файл усередині git-репо. Тека, яка стала репо пізніше, клон на іншій машині або вже закомічений файл лишаються без захисту. У `.gitignore` самого репо правило не потрапляє.

Apiiro переглянула всі 104 185 публічних копій цього файлу на GitHub. У 1 122 файлах лежить справжній секрет: паролі до баз, ключі Supabase, AWS, npm і GitHub, 43 логіни SSH. З історією git, спільними `settings.json` і транскриптами агентів набралось 2 539

секретів у 1 994 репо. У 539 з 1 105 репо файл змінював коміт, співавтором якого стоїть сам Claude.

Сканери ловлять це погано. gitleaks знайшов 564 з 1 122 файлів, TruffleHog знайшов 643, а 215 файлів не знайшов жоден.

Причина: пароль після `PGPASSWORD=` чи `sshpass -p` не має впізнаваного формату ключа. Користувачі повідомляли про механіку в issues з серпня 2025 року, відповіді від Anthropic там нема.

Чому це важливо: кнопка «більше не питати» перетворює одноразовий дозвіл на постійний запис на диску. Практичний захист короткий. Додайте `.claude/settings.local.json` у `.gitignore` кожного репо, передавайте секрети через змінні середовища і дозволяйте шаблони команд замість дослівних рядків. Якщо файл колись потрапив у коміт, міняйте ключі: видалення файлу не чистить історію і форки.

ТЕМА 2

MaxxBench: малі зміни вимог розводять «рівні» моделі на 23 пункти

ДЖЕРЕЛА MaxxBench, 20.10 Unlap · @loresjpg, 07.11 @loresjpg · HN, 07.11 Hacker News

Брати Гевін і Джастін Ло взяли 89 задач з DeepSWE і змінили в кожній одну дрібницю. Наприклад, імена файлів звітів тепер мають бути малими літерами, а час у відповіді API має бути в UTC. Медіанний еталонний патч виріс лише на 17 рядків, тобто на 3,5%.

Результат сильний. Claude Opus 5.5 і Gemini 3.8 Flash мають на DeepSWE близько 74%. На MaxxBench Opus 5.5 дає 76,4%, а Gemini 3.8 Flash дає 53,4%. DeepSeek V4.1 Flash падає з 74,2% до 55,6%. Розкид між 15 конфігураціями виріс з 20,9 до 48,3 пункту.

Автори описують і поведінку. Модель розуміла нову вимогу, а потім вирішувала, що приховані тести хочуть старого варіанту. В одному прогоні модель правильно все реалізувала, спитала іншу модель про оригінальну відповідь і видалила власний правильний код. Пост Джастіна Ло зібрав понад 500 тисяч переглядів, його перепостив Гаррі Тан.

Чому це важливо: популярний бенчмарк з часом міряє, наскільки модель вивчила саме його. Для вибору моделі під реальну роботу корисніший такий тест: та сама задача, але з правкою, яку зробив би рецензент. Різниця в 23 пункти між моделями з однаковим балом важить більше за будь-який рядок у таблиці лідерів.

ТЕМА 3

Microsoft закрила групу AI Frontiers, її засновник пішов

ДЖЕРЕЛА John Langford, 06.11 Hunch · HN, 07.11 Hacker News

Джон Ленгфорд, один з відомих теоретиків машинного навчання, написав, що AI Frontiers більше нема. Групу на ~50 людей у Microsoft Research створили 2023 року. Вона зробила фреймворк Autogen, агента Fara для керування комп'ютером і дослідження нових архітектур.

На початку вересня групу перевели в Microsoft AI. За словами Ленгфорда, керівництво MAI з колишньої Inflection ставить на масштабування і «агресивно не на дослідження». Він пише, що там групу «просто не хотіли». Ленгфорд пішов, і, за його словами, так само вирішили всі інші засновники AIF. Стажувань з цією командою наступного року не буде.

Свій аргумент він дає з цифрою. Експерименти ByteDance показують, що варіант його Full Bandwidth Transformer працює на рівні моделі вдвічі більшого розміру. Це половина вартості тренування й інференсу за ту саму якість.

Чому це важливо: великі лаби дедалі частіше обирають масштаб замість досліджень, бо віддачу від масштабу легше планувати. Дослідники, які думають інакше, тепер ідуть у менші команди. Від того, куди вони підуть, залежить, звідки прийде наступна економія на обчисленнях.

ТЕМА 4

На кожному Mac працює граф знань про власника і його родину

ДЖЕРЕЛА The Eighth Rank, 28.10 8rank · HN, 07.11 Hacker News

Дослідники Даріо Паскуїні і Міхал Базилі розібрали два демони macOS: `knowledgeconstructiond` і `intelligenceplatformd`. Вони працюють з macOS 13 (2022) і будують граф про користувача. Офіційний опис займає кілька рядків у man-сторінці.

У `~/Library/IntelligencePlatform` лежить 51 база SQLite у відкритому вигляді. Доступ до неї закриває лише дозвіл Full Disk Access. Головна база `graph.db` має 181 клас сутностей і 278 типів зв'язків. У граф ідуть контакти, обличчя з Photos, календар, Family Sharing з віком кожного члена родини, екстрений контакт з Health і дані з пошти й повідомлень.

Найцікавіша частина: два класифікатори XGBoost вирішують, хто з контактів родина. Вони беруть 144 ознаки, і більшість з них поведінкові: з ким людина листується і з ким з'являється на фото, з розбивкою за днем тижня і часом доби. Одна з ознак зветься `photosPersonPosteriorProbabilityGivenSaturdayNight`. Автори відкрили локальний дашборд iKnow, щоб кожен міг подивитись свій граф.

Чому це важливо: персональний AI потребує контексту, і цей контекст хтось має зібрати. Тут його зібрала ОС, без окремої згоди людей, які потрапили в граф. Для оцінки ризику важливе одне питання: що станеться, якщо такий файл опиниться в чужих руках. Відповідь залежить лише від одного дозволу на диск.

ТЕМА 5

Справа Хуанга: FT пише про пам'ятку розвідки, сенатор обіцяє розслідування

ДЖЕРЕЛА Financial Times, 07.11 FT [одне джерело]

Вчора згадували, що три комітети Палати представників запросили Дженсена Хуанга на закритий брифінг. Сьогодні FT додає деталь. За даними джерел видання, посадовці США цього року написали пам'ятку на основі даних розвідки. У ній сказано, що Хуанг мав романтичні стосунки з Еліс Хуанг, керівницею сінгапурської Megaspeed.

Розвідка США, пише FT, вважає, що Еліс Хуанг завербувало Міністерство державної безпеки Китаю. Пам'ятку отримали кілька топ-посадовців перед поїздкою Трампа на саміт із Сі Цзіньпіном. Білий дім і ЦРУ відмовились від коментарів. Nvidia не коментує пам'ятку і раніше казала, що Хуанг зустрічає «тисячі керівників клієнтів щороку».

Сенатор Кріс Кунс, який з січня очолить комітет Сенату з закордонних справ, пообіцяв розслідування. Megaspeed уже перевіряють через можливу контрабанду чипів Nvidia в Китай. Внутрішня перевірка Nvidia порушень не знайшла.

Чому це важливо: історія вийшла за межі експортного контролю і тепер стосується особистої безпеки керівника найдорожчої AI-компанії. Обидві палати Конгресу тепер мають до Nvidia окремі питання. Усе, крім заяви Кунса, поки спирається на анонімні джерела FT.

ТЕМА 6

Будівництво дата-центрів упирається в електрику і воду

ДЖЕРЕЛА The Guardian, 07.11 Guardian · The Guardian, 07.11 Guardian · Financial Times, 07.11 FT

Таїланд у вересні призупинив будівництво 49 дата-центрів і рішення ще по 117 проєктах. На початку року країна схвалила проєкти TikTok, Skyline і Bridge на $27 млрд. У малайзійському Джохорі потужність дата-центрів виросла з 94 МВт у 2023 році до 1 110 МВт у 2026 році. За оцінкою Wood Mackenzie, дата-центри вже беруть 24% електрики штату, а до 2035 року можуть брати 40%. У лютому в Джохорі пройшов перший протест проти такого будівництва.

У Шотландії DataVita обіцяла живити кампус на 1 ГВт біля Глазго від відновлюваних джерел. Після питань Guardian компанія переписала план: кампус буде «fully grid served». При цьому проєкт отримав £202 млн державних гарантій. FT того ж дня цитує міністра економічного зростання Британії: країна не сповільнить AI, попри негативну реакцію в США.

Чому це важливо: обмеження для AI зараз фізичні: мережа, вода і згода місцевих громад. Країни, які рік тому змагались за дата-центри, тепер рахують, хто платить за

електрику. Обіцянки «зеленої» енергії в заявках варто перевіряти так само, як цифри в бенчмарках.

ТЕМА 7

Практики знімають зайві запобіжники: моделі вже кращі за них

ДЖЕРЕЛА @garrytan, 07.11 @garrytan · @emollick, 07.11 @emollick · @emollick, 07.11 @emollick · @dexhorthy, 07.11 @dexhorthy

Гаррі Тан пише, що скілам для агентів потрібен цикл з евалами. Кожна нова модель краща, тому зайве можна викидати. Він сам видалив скіл `/investigate`, бо Opus 5.5 робить цю роботу краще без нього.

Ітан Моллік вважає, що страх перед фактичними помилками AI у щоденній роботі застарів. За його словами, дані про нові моделі показують: вони краще за людей-експертів, включно з PhD, знаходять факти і перевіряють твердження. Окремим постом він пише, що LLM можуть у 10 разів прискорити розслідувальну журналістику. Смак до того, яка історія цікава, поки лишається людським.

Декс Хорті додає технічну деталь: компакція контексту стала значно кращою. Для частини задач контекст більше не треба вручну чистити заради якості роботи моделі.

Чому це важливо: кожен запобіжник має ціну, і з новою моделлю частина з них стає зайвою. Перевіряти це варто евалом. Пункт 1 показує зворотний бік: запобіжник «спитати перед командою» прибрала кнопка, а наслідки лишились на диску.

ТЕМА 8

Discord на Rust: клієнт стартує одразу і бере на 70% менше пам'яті

ДЖЕРЕЛА Windows Latest, 06.11 Windowslatest · HN, 07.11 Hacker News

Технічний директор Discord Станіслав Вишневський показав 15-секундне відео. Новий клієнт на Rust і поточний клієнт на Electron стартують поруч на двох ноутбуках з Windows 11. Новий клієнт показує список друзів раніше, ніж старий проходить екран завантаження. Новий клієнт займає 290,2 МБ пам'яті з двома акаунтами одночасно. Співробітники Discord підтвердили, що обидва клієнти стартували з холодного запуску.

Чому це важливо: Electron роками був розумним компромісом: один код на всі платформи. Тепер переписати великий клієнт стало дешевше, зокрема завдяки агентам для коду. Тому аргумент «зручно розробникам» слабшає проти аргументу «швидко користувачам».

ТЕМА 9

Unitree: роботів збирають руками, і це економічно правильно

ДЖЕРЕЛА Josef Chen, 07.11 Josef · HN, 07.11 Hacker News

Засновник KAIKAKU відвідав фабрику Unitree в Ханчжоу. У цеху актуаторів стоять одна-дві автоматичні лінії, решту роботи роблять люди на старих намотувальних верстатах. Вірусне відео з гуманоїдом на складанні проспект IPO називає пілотом, а складання «currently mainly manual».

Цифри з проспекту прості. Наприкінці 2025 року все обладнання Unitree коштувало близько $1,7 млн при майже 32 000 роботів за рік, тобто ~$50 обладнання на робота. Праця становила 8% собівартості. Три чверті доходу від гуманоїдів за 9 місяців 2025 року дали дослідження й освіта, менше 5% дали заводи.

Чому це важливо: гуманоїди поки купують переважно лабораторії. Автоматизація збирання економить мало, коли праця становить 8% вартості. Справжнє обмеження в «мозку» робота, і сам гендиректор Unitree тепер робить ставку саме туди.

ТЕМА 10

Ставки на Polymarket за годину до опитування NYT

ДЖЕРЕЛА The New York Times, 06.11 NYT [одне джерело]

Дослідники з Університету Вандербільта знайшли підозрілі ставки перед двома опитуваннями NYT/Siena. Один користувач Polymarket 31.10 поставив $191 277 на перемогу сенатора Піта Рікеттса в Небрасці. Приблизно за годину вийшло опитування з перевагою Рікеттса в 6 пунктів. Користувач заробив понад $77 000.

Той самий користувач поставив $622 608 на перемогу демократа в Мічигані, і наступного дня інше опитування показало таку перевагу. Прибуток склав понад $180 000. Дослідники не стверджують інсайду: людина могла вгадати лише час публікації або хеджувати інші позиції.

Чому це важливо: ринки прогнозів продають «чисту» ймовірність, але вони чутливі до будь-якого витоку інформації.

Будь-яка організація, що публікує дані за розкладом, тепер має окремий ризик: її розклад сам стає торговою інформацією.

---

misc

- **Масштаб розпродажу AI:** Kadoa порівняла поточне падіння з відомими крахами. S&P 500 на 6% нижче рекорду, Nasdaq на 11%, а індекс чипів на 36%, стільки ж, як у Covid (35%). Kadoa · HN Hacker News
- **Робота і AI:** за даними WSJ, у жовтні професійні й бізнес-послуги в США додали 70 000 робочих місць, найбільше з липня 2022 року. Юристи, консультанти і бухгалтери теж наймали. WSJ

- **Натрій-іонні батареї:** Wood Mackenzie чекає паритету вартості з LFP на рівні комірки до кінця 2026 року. Угоди на постачання вже перевищують 70 ГВт·год. Pv-magazine · HN Hacker News
- **Меблі з агентом:** @levelsio пише, що Claude Code з FreeCAD проєктує меблі по деталях і дає список матеріалів. Його оцінка: до 85% економії проти преміальних брендів. @levelsio
- **TristanTube:** @karpathy за 3 хвилини зібрав з Claude Code каталог на 47 000 технічних відео за списком Трістана Хьюма. @karpathy
- **Нова сторінка PR на GitHub:** GitHub відкрив опційний огляд PR зі статусом мержу і наступними діями зверху сторінки. Github · HN Hacker News
- **Спадкоємці засновників Anthropic:** Тайлер Коуен розбирає схему Founder LLC. Кожен з 7 співзасновників веде список до 10 можливих спадкоємців свого голосу, і 5 з 6 інших мають його схвалити. Marginal Revolution
- **Саттон проти чистого масштабу:** Річард Саттон написав, що грубої сили обчислень замало для інтелекту. @amasad назвав це «The Better Lesson». @amasad

---