Для кібератак на Україну росіяни намагалися використати Claude, - Anthropic

22:30 11.09.2026 Пт 2 хв

Штучний інтелект сам переписував код, аби обійти захист

СЕРГІЙ КОЗАЧУК

Фото: для кібератак проти України РФ використала ШІ Claude (Getty Images)

Російські хакери намагалися використати штучний інтелект Claude від компанії Anthropic для проведення кібератак проти українського уряду, військових та дипломатичних структур.

Про це повідомляє РБК-Україна з посиланням на Reuters.

Компанія Anthropic оприлюднила звіт Threat Intelligence, у якому задокументувала зловживання своїми технологіями штучного інтелекту за останні вісім місяців.

За даними розробників, зловмисники активніше **використовують ШІ для організації кібератак**, залишаючи людям лише функцію наглядачів.

Як хакери атакували Україну

Підтримувана державою-агресоркою хакерська група використовувала моделі Claude майже на кожному етапі своїх операцій. Вони проводили фішингові розсилки, перехоплювали дані Wi-Fi у готелях та отримували доступ до облікових записів у WhatsApp.

Усі ці атаки спрямовувалися проти посадовців урядового, військового та дипломатичного секторів України.

Використовуючи можливості ШІ, зловмисники створили систему, яка автоматично виявляла блокування шкідливого коду антивірусами та переписувала його доти, доки він не ставав "невидимим" для засобів захисту.

Аналітики зазначають, що тактика цієї групи відповідає діяльності російського угруповання Midnight Blizzard, яке пов'язують із Службою зовнішньої розвідки РФ.

Не лише хакерство, а й зброя та витік даних

Крім кібератак на Україну, компанія виявила й інші загрози:

- **Розробка зброї** - Користувачі з Росії, Китаю та Ємену намагалися використовувати Claude для створення програмного забезпечення для вогнепальної зброї, ракет, бойових безпілотників та систем наведення.
- **Спроби розробки біозброї** - Фахівці заблокували кілька акаунтів, де дослідники намагалися спланувати експерименти з адаптації ссавців до пташиного грипу.
- **Атаки на китайських конкурентів** - Сім китайських лабораторій (зокрема Alibaba, Moonshot та DeepSeek) здійснювали масові атаки, щоб перехопити відповіді Claude і використати їх для навчання власних моделей ШІ.

Усі виявлені акаунти зловмисників було заблоковано, а отримані дані використано для посилення захисту продуктів Anthropic.

Російські хакери атакують Україну

Нагадаємо, це не перший випадок, коли російські хакери використовують технологічні уразливості для атак на українські структури.

Нещодавно кіберзлочинці з РФ знайшли спосіб "засліпити" захист штучного інтелекту під час атак на українські організації.

Техніка під назвою GuardBreaker змушувала мовні моделі відмовлятися від перевірки файлів, через що російські хакери "ламали" ШІ-захист і залишали шкідливе програмне забезпечення непоміченим під час атак на енергетику та транспорт.

Крім того, фахівці Google Threat Intelligence Group виявили шпигунський .NET-бекдор STOCKSTAY.

За допомогою цієї програми російські хакери атаковували урядові структури та військові відомства України, а також європейські дипломатичні установи, маскуючи вірус під легітимні утиліти.

Більше по темі:
Кібератака | Україна | Російська Федерація | Штучний інтелект

НОВИНИ

Окупанти під Добропіллям стратили полонених нацгвардійців

АНАЛІТИКА

Костянтин Широкун
кореспондент РБК-Україна

Українські КАБи запускатимуть дрони: інтерв'ю з CEO BlueBird Tech

НОВИНИ
Новини України
Війна в Україні
Економіка
Світ
Надзвичайні події
ПОЛІТИКА
АНАЛІТИКА
Статті
Інтерв'ю
Точка зору
БІЗНЕС
Економіка
Фінанси
Авто
Tech
Енергетика
Біла економіка
ЖИТТЯ
Гроші
Зміни
Освіта
Суспільство
СПОРТ
Футбол
Баскетбол
Теніс
Бокс
STYLER
Люди
Тренди
Корисне
Смачно
Гороскопи
WAVE
Інсайдер
Стиль
Велнес
Культура
Подорожі
Смак
Зірки
РБК-УКРАЇНА UA | EN | RU
Про компанію
Редакційна політика і стандарти
Як стати нашим автором
Правила користування
Правова інформація
Політика конфіденційності
Контакти
Команда
Вакансії в РБК-Україна
Розмістити рекламу

Ідентифікатор онлайн-медіа в Реєстрі суб’єктів у сфері медіа — R40-05347