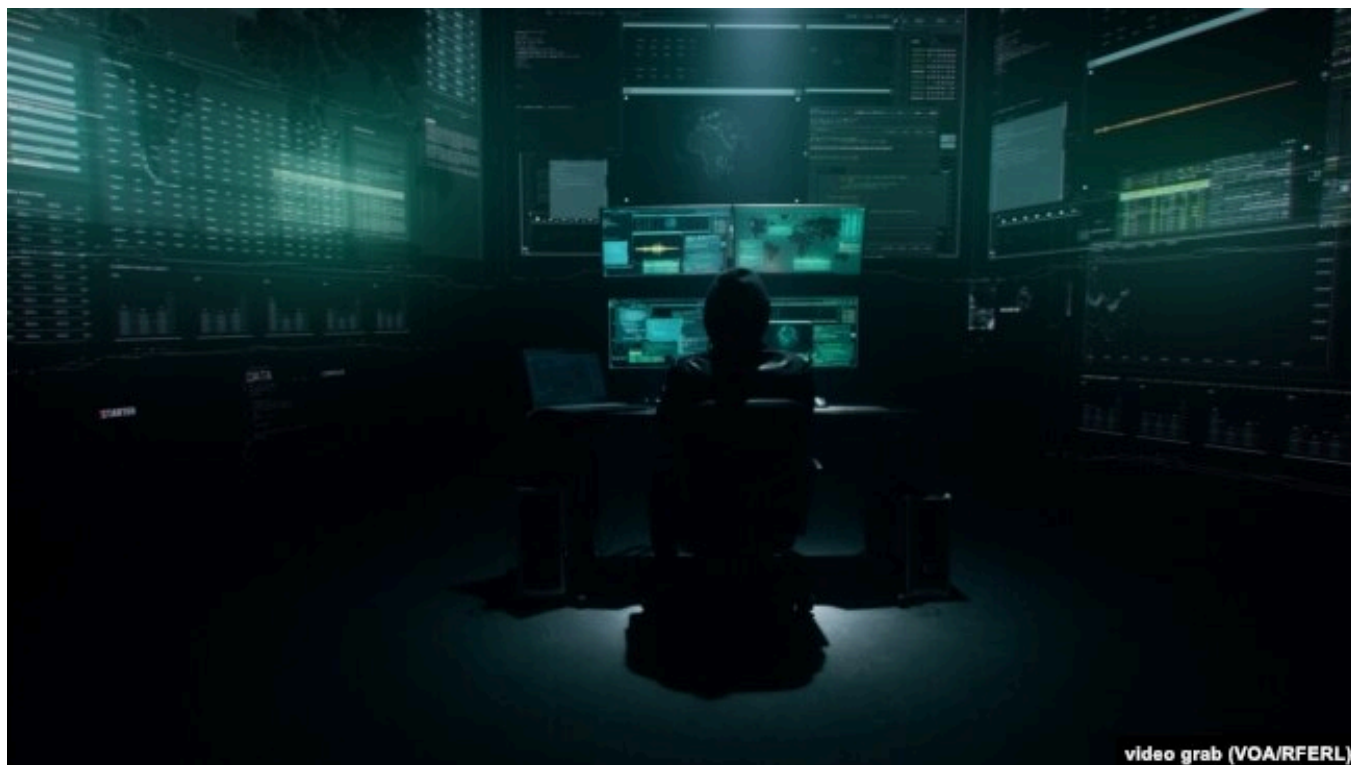


Русскоговорящих хакеров заподозрили в обмане ИИ-агента SpaceX

менее минуты назад

 Приоритетный источник в Google



video grab (VOA/RFERL)

Русскоговорящие хакеры использовали ИИ-агента Cursor (редактор кода на базе искусственного интеллекта) компании SpaceX, чтобы взломать бельгийскую химическую компанию и как минимум шесть других фирм за последние несколько месяцев. Об этом в четверг сообщает [Reuters](#) со ссылкой на отчет компании Gambit Security, специализирующейся на кибербезопасности.

В Gambit отметили, что действия хакеров удалось раскрыть после того, как они оставили незащищенным доступ к серверу, через который работали с Cursor. Как следует из сообщения, речь идет о новой группировке под названием AurOra, распространяющей программы-вымогатели.

В своем отчете Gambit указала, что AurOra убедила ИИ-агента выполнить сотни вредоносных операций - например, кражу учетных данных или захват ценных аккаунтов, - ложно утверждая, что этот взлом является частью симуляции.

Череда кибератак с использованием искусственного интеллекта - это очередной пример того, как злоумышленники применяют коммерческие ИИ-инструменты для проникновения в системы, пишет Reuters. По словам директора по стратегии компании Gambit Кертиса Симпсона, это также демонстрирует, что разработчики ИИ-решений вовлечены в бесконечную "гонку вооружений" с недобросовестными пользователями, пытающимися обойти встроенные механизмы защиты.



СМОТРИ ТАКЖЕ

OpenAI обнаружила новые случаи выхода ИИ-моделей из-под контроля

Gambit не стала приводить названия пострадавших от действий хакеров структур, однако агентству Reuters удалось установить шесть из них после самостоятельного анализа части данных. В списке агентства, в частности, указаны бельгийская компания Christeys (производитель средств гигиены и чистящих средств из Гента), немецкий производитель гаражных ворот Teckentrup и шотландская организация Helideck Certification Agency, занимающаяся сертификацией вертолетных площадок.

Компания SpaceX на запросы о комментариях не ответила.

Этот контент также в категориях

Новости - мир

Новости