

Исследователи из компании Okta заявили, что хакеры начали использовать генеративный ИИ-сервис v0 от Vercel для создания фишинговых сайтов — в том числе клонов страницы входа login.okta.com. На генерацию таких страниц у злоумышленников уходит менее 30 секунд.

По словам представителей Okta, это первый зафиксированный случай, когда ИИ использовался не для написания текста фишингового письма, а для создания полной инфраструктуры атаки.

В демонстрации, представленной журналистам Axios, фальшивый сайт создавался по простому текстовому запросу: «Сделай копию login.okta.com». Хотя подтверждений успешной кражи учетных данных пока нет, Okta обнаружила и другие поддельные сайты, нацеленные на пользователей Microsoft 365 и криптосервисов.

Vercel уже удалил вредоносные ресурсы и работает над системой жалоб и автоматического обнаружения подобных злоупотреблений.

Однако исследователи обнаружили, что выложенные на GitHub клоны v0 позволяют хакерам продолжать атаки даже в случае блокировки оригинальной платформы.