DEEPFAKE CORAZ POPULARNIEJSZY WŚRÓD PRZESTĘPCÓW

Cyberprzestępcy wykorzystują coraz częściej w swojej pracy technologie deepfake do podszywania się pod inne osoby. Ich liczba wzrosła w ciągu roku dwukrotnie - alarmują eksperci z firmy TestArmy CyberForces.

Według związanego z firmą Wojciecha Liki "najnowocześniejsze algorytmy potrzebują zaledwie jednego zdjęcia i pięciosekundowej próbki głosu, aby wygenerować niemalże identyczny hologram deepfake, którego odróżnienie od pierwowzoru bez użycia specjalistycznych metod jest praktycznie niemożliwe".

Zdaniem specjalistów z TestArmy CyberForces pierwsze algorytmy tego typu pojawiły się w końcu 2017 roku. Od tego czasu wykorzystywane są głównie przez branżę pornograficzną. Problem zaczyna jednak w opinii ekspertów sięgać dużo głębiej, a liczba materiałów w technologii deepfake, jakie znaleziono w internecie rośnie z 7964 nagrań w 2018 roku do 14,6 tys. w roku 2019.

12 proc. nagrań deepfake ma uderzać według specjalistów w polityków, 5 proc. w dziennikarzy, a 2 proc. w osoby z kręgów biznesowych. Statystyka ta pomija filmy deep fake o charakterze pornograficznym. Jednocześnie firma informuje, iż wykryła 20 niezależnych portali internetowych, które są odpowiedzialne za wytwarzanie materiałów w tej technologii. Treści z ich użyciem wygenerowało 96 tys. unikalnych użytkowników, którzy zarejestrowali swoje konta w tych witrynach.

Firma zwraca uwagę, że zjawisko deepfake może stanowić zagrożenie również dla osób spoza życia publicznego i stać się bronią skierowaną przeciwko dochodowym firmom i wpływowym przedsiębiorcom, np. służąc do wyłudzania środków finansowych.

Eksperci doradzają, by chcąc chronić się przed deepfake'ami stawiać na edukację poświęconą zagrożeniom związanym z tą technologią. Istotne jest również korzystanie z narzędzi specjalistycznych, które firmy i organizacje mogą wykorzystywać do rozpoznawania algorytmów deepfake i ich wytworów. Przykładowo, oprogramowanie takie jak Sherlock AI pozwala wykryć anomalie w filmach wideo, a Natural Hash umożliwia osadzanie w materiałach źródłowych nieedytowalnych cyfrowych znaków wodnych, które mogą zabezpieczać przed modyfikacjami nagrań