**Stany Zjednoczone, Polska i inne kraje obawiają się deepfake podczas tegorocznych wyborów. Fałszywe filmy już można kupić na Telegramie!**

**W 2024 roku wybory odbędą się w niemal 70 krajach świata, których łączna populacja sięga połowy ludzkości. Przyszłość demokracji wisi jednak na włosku za sprawą deepfake. Technologia ta już teraz wykorzystywana jest do manipulowania opinią publiczną – ostrzegają eksperci Check Point Research, dodając, że usługi deepfake są szeroko oferowane zarówno w darknecie, jak i na kanałach Telegram.**

**W czasach, gdy innowacje cyfrowe wywierają głęboki wpływ na każdy aspekt naszego życia, integralność procesów demokratycznych stoi na rozdrożu. Współczesna era zapoczątkowuje nie tylko postęp technologiczny, ale także wyrafinowany mechanizm oszustwa, który może podważyć podstawy demokracji. Państwa na całym świecie przygotowują się do nadchodzących wyborów, jednak stajemy w obliczu nowego i bezprecedensowego ryzyka, które wykracza poza zwykłe nadużycia technologiczne**

**Przeprowadzone przez Check Point Research badania ujawniają gwałtowny wzrost dostępności usług deepfake w darknecie i na Telegramie. Zjawisko to nie jest dziełem tzw. „samotnych wilków”, ale skoordynowanym działaniem sieci oszustów i hakerów, którzy nie pozostawiają cyfrowych śladów i działają bezkarnie za swoimi ekranami. Ich działania tworzą złożoną siatkę dezinformacji i manipulacji, co znacznie komplikuje wysiłki na rzecz ochrony integralności wyborów i utrzymania zaufania społeczeństwa do procesu demokratycznego.**

**Wyzwanie Deepfake**

Technologia Deepfake pozwala na tworzenie hiperrealistycznych, ale sfabrykowanych treści audiowizualnych, oferując potężne narzędzie dla tych, którzy chcą manipulować opinią publiczną lub dyskredytować polityków. Prostota dostępu do tych usług i korzystania z nich podkreśla rosnące zagrożenie nie tylko dla uczciwości i przejrzystości wyborów, ale także dla podstawowego zaufania, na którym zbudowane są instytucje demokratyczne.

**Rynek AI deepfake odnotowuje niezwykły wzrost. Analitycy firmy MarketandMarket szacują jego wartość na 7 mld dolarów w 2024 r. i ma ona wzrosnąć do 38,5 mld dolarów w 2030!**

Z przeglądu ekspertów Check Pointa wynika, że na platformach takich jak GitHub istnieje ponad 3000 repozytoriów związanych z technologią deepfake, co wskazuje na jej szeroki potencjał rozwoju i dystrybucji. Telegram obsługuje setki kanałów (około 400–500) i grup oferujących usługi deepfake, począwszy od automatycznych botów prowadzących użytkowników przez proces po spersonalizowane usługi świadczone bezpośrednio przez konkretne osoby. Ich ceny są zróżnicowane i zaczynają się od 2 dolarów za film, a kończą na 100 dolarów w przypadku wielu filmów i korekt, co sprawia, że zamawianie zwodniczych treści jest niepokojąco przystępne.

Aby w pełni zrozumieć bezpośrednie zagrożenie, jakie stwarza technologia deepfake podczas nadchodzących wyborów w USA w 2024 r., należy uznać, że nie jest to wyłącznie wyzwanie wynikające z zaawansowania technologicznego, ale przejaw szerszego, bardziej podstępnego mechanizmu oszustwa. Za ekranami działa podziemna sieć aktorów zagrożeń, wykorzystujących te technologie nie tylko jako narzędzia, ale jako broń w kompleksowej strategii mającej na celu podważanie integralności demokracji. Ten tajemniczy mechanizm, zaaranżowany kilkoma kliknięciami, manipuluje opinią publiczną z przerażającą skutecznością… jednocześnie jego sprawcy pozostają anonimowi i nie pozostawiając praktycznie żadnych cyfrowych śladów.

Wg analityków Check Point Research problem ten komplikuje zwalczanie tego typu praktyk. Tradycyjne środki cyberbezpieczeństwa nie sprawdzają się, gdy nie ma wyraźnych „odcisków”, za którymi można podążać – np. adresów IP do wpisania na czarną listę lub prostych sygnatur złośliwego oprogramowania do wykrycia. Pole bitwy przesuwa się zatem z technicznych środków zaradczych na bardziej złożoną arenę wojny psychologicznej i świadomości społecznej.

Prawdziwym zagrożeniem jest zatem nie tylko technologia, ale cały ekosystem oszustwa, który ona umożliwia. Działa on poprzez skomplikowaną sieć botów, fałszywych kont i anonimowych usług, a wszystko to zaprojektowane jest w celu tworzenia, wzmacniania i rozpowszechniania sfabrykowanych treści. To forma wojny partyzanckiej w epoce cyfrowej, w której napastnicy, niewidzialni i nieuchwytni, manipulują nie tylko informacjami, ale samą strukturą rzeczywistości postrzeganą przez elektorat.

Jednym z niedawnych [przykładów](https://www.npr.org/2024/01/22/1226129926/nh-primary-biden-ai-robocall) złośliwego zastosowania deepfake było automatyczne połączenie telefoniczne z wyborcami w New Hampshire z fałszywym głosem prezydenta USA Joe Bidena i informującym wyborców, aby nie oddawali swojego głosu. - Chociaż głos w automatycznej rozmowie brzmi jak prezydenta Bidena, na podstawie wstępnych danych wydaje się, że wiadomość ta została sztucznie wygenerowana – podało biuro AG w [oświadczeniu](https://www.doj.nh.gov/news/2024/20240122-voter-robocall.html).

W związku z tym wydarzeniem i upowszechnieniem klonowania głosu, Stany Zjednoczone [zakazały automatycznych połączeń](https://www.ndtv.com/world-news/deepfakes-artificial-intelligence-joe-biden-us-bans-ai-powered-voice-robocalls-heres-why-5042584)głosowych generowanych przez sztuczną inteligencję.

*- Atakujący (*ang. bad actors - przyp. red*.) wykorzystują głosy generowane przez sztuczną inteligencję w niezamówionych automatycznych połączeniach, aby dokonywać wyłudzeń od bezbronnych członków rodziny, naśladować celebrytów i wprowadzać w błąd wyborców. Zwracamy uwagę na oszustwa stojące za tymi automatycznymi połączeniami* – stwierdziła Federalna Komisja ds. Komunikacji.

Gdy przeanalizujemy wpływ deepfakes na wybory w USA w 2024 r., staje się jasne, że ochrona procesów demokratycznych w epoce cyfrowej wymaga wieloaspektowego podejścia. Dotyczy to nie tylko działań legislacyjnych, ale także świadomości społecznej, rozwiązań technologicznych i współpracy międzynarodowej. Wyzwanie polega nie tylko na zwalczaniu samej technologii, ale także na utrzymaniu zaufania niezbędnego w społeczeństwach demokratycznych.

Pojawienie się technologii deepfake jako narzędzia ingerencji w wybory podkreśla krytyczny moment dla demokracji na całym świecie. W miarę zbliżania się wyborów w 2024 r. w wielu krajach na całym świecie, w Azji, Europie i USA, potrzeba zachowania czujności i proaktywnych działań nigdy nie była bardziej nagląca – ostrzegają specjaliści bezpieczeństwa cybernetycznego z Check Point Research.