

Wielkie firmy „podśluchują” wyłączonymi mikrofonami

27 kwietnia 2022

Zgodnie z nowym, jeszcze nieopublikowanym, badaniem z Uniwersytetu Wisconsin-Madison jeśli zauważyłeś w przeszłości, że wyświetlają ci się reklamy oparte na czymś, o czym być może wspominałeś znajomemu lub współmałżonkowi i myślałeś, że to tylko zbieg okoliczności, to się mylisz.

Według komunikatu prasowego instytucji naukowcy twierdzą, że zbadali „wiele popularnych aplikacji”, aby określić, jakie dane są w stanie przechwycić, nawet gdy użytkownik ma wyciszony mikrofon na swoim urządzeniu. W komunikacie prasowym nie wspomniano, które aplikacje zostały zbadane, ale to, co odkryli naukowcy, jest wystarczająco potępiające, że ich badanie zostało według Reclaim The Net zaakceptowane na sympozjum Privacy Enhancing Technologies Symposium 2022.

„Wykorzystali narzędzia do analizy binarnej środowiska uruchomieniowego, aby śledzić nieprzetworzony dźwięk w popularnych aplikacjach do wideokonferencji, gdy dźwięk przemieszczał się z aplikacji do sterownika audio komputera, a następnie do sieci, gdy aplikacja była wyciszona” – napisano w komunikacie prasowym. „Odkryli, że wszystkie testowane przez nich aplikacje od czasu do czasu zbierają nieprzetworzone dane dźwiękowe, gdy nagrywanie dźwięku jest wyłączone, przy czym jedna popularna aplikacja zbiera informacje i dostarcza dane na swój serwer w tym samym tempie, niezależnie od tego, czy mikrofon jest wyciszony, czy nie”.

Z pomocą sztucznej inteligencji (AI), a także uczenia maszynowego, wielkie technologiczne firmy są w stanie wykorzystać surowe dane audio w celu wyciągnięcia dokładnych wniosków na temat użytkowników. Naukowcy biorący udział w badaniu wykorzystali technologie, aby zobaczyć, jakie wnioski

mogą wyciągać te firmy i stwierdzili, że są one dość trafne.

Według streszczenia badania uzyskanego przez „The Next Web”: „Korzystając z przechwyconego ruchu sieciowego w drodze do serwera telemetry, wdramy klasyfikator aktywności w tle typu „proof-of-concept” i demonstrujemy wykonalność wnioskowania o trwającej aktywności w tle podczas spotkania – gotowanie, sprzątanie, pisanie na klawiaturze itp. Osiągnęliśmy 81,9% makro dokładności podczas identyfikowania sześciu typowych czynności wykonywanych w tle przy użyciu przechwyconych wychodzących pakietów telemetrycznych, gdy użytkownik był wyciszony”.

Innymi słowy, studenci studiów magisterskich na uniwersytecie byli w stanie odkryć, co użytkownik aplikacji do wideokonferencji robi w tle, podczas gdy mikrofon ich urządzenia był wyciszony i byli trafni w 80 procentach. „Jeśli chodzi o kamerę to możesz ją wyłączyć, a nawet położyć na nią rękę i bez względu na to, co robisz, nikt cię nie zobaczy. Nie sądzę, że to samo można zrobić z mikrofonem” – powiedział główny autor badania, Kassem Fawaz.

Krótko mówiąc, wielkie firmy technologiczne zdecydowały, że bez względu na wszystko, nie muszą przestrzegać rzekomych gwarancji prywatności zawartych w Czwartej Poprawce do Konstytucji Stanów Zjednoczonych, aby mogły stale sprzedawać ci towary i usługi, a także pozyskiwać głęboko prywatne informacje, które mogą być później wykorzystane do szantażowania cię – i robią to za wiedzą i na polecenie federalnego rządu.

Teraz wiesz, dlaczego Kongres odmawia podjęcia walki z wielkimi firmami technologicznymi: prawdopodobnie te firmy mają wszystkie dobra dla każdego członka i grożą ujawnieniem każdemu, kto sprzeciwia się ich przejęciu władzy.

Jeden z ustawodawców, republikanin z Florydy, Matt Gaetz, niedawno wypowiedział się na ten temat, zauważając, że jego

koledzy nie powstrzymują tych wielkich firm, ponieważ są opłacani przez „właścicieli” tych firm. „Kongres nie powstrzyma Big Techu, ponieważ Kongres jest kupiony przez Big Tech” – powiedział Gaetz we wrześniu 2020 r., kiedy platformy cenzurowały potępiające informacje na temat kandydata na prezydenta Demokratów Joe Bidena. „Jest po prostu zbyt wielu członków Izby Reprezentantów i Senatu, którzy należą do Big Techu albo z powodu darowizn politycznych, albo dlatego, że członkowie ich rodzin są zatrudniani przez te firmy” – dodał.

Autorstwo: JD Heyes

Na podstawie: [TheNextWeb.com](https://thenextweb.com), [ReclaimTheNet.org](https://reclaimthenet.org), [Wisc.edu](https://wisc.edu)

Źródło oryginalne: [NaturalNews.com](https://naturalnews.com)