

Ukryte ultradźwiękowe sygnały w reklamach telewizyjnych sterują smartfonami by śledziły właścicieli

11 maja 2017

Zdaniem niemieckich badaczy ukryte sygnały nadawane w reklamach telewizyjnych mogą sterować smartfonami by szpiegowały swoich właścicieli za pomocą nasłuchującego oprogramowania.

Ostatnio odnotowano ogromny wzrost aplikacji na Androida używających oprogramowanie przeznaczone do wyszukiwania niesłyszalnych sygnałów „ultradźwiękowych”. Sygnały te mogą zawierać kod, który nakazuje programom śledzenie lokalizacji osób, tego co oglądają w telewizji, a nawet gromadzenie informacji osobistych, takich jak przynależność polityczna i pornografia, ostrzegają badacze.

Oprogramowanie Silverpush ma służyć do słuchania „sygnałów dźwiękowych”, których ludzie nie słyszą. Było ono używane przez korporacje takie jak m.in. McDonald's i Krispy Kreme.

Aplikacje, które używają tego oprogramowania, mogą „precyzyjnie łączyć oglądanie nawet wrażliwych treści, takich jak filmy dla dorosłych lub dokumenty polityczne z konkretną osobą – nawet w różnych lokalizacjach” – stwierdzili naukowcy. „Reklamodawcy mogą wnioskować o tym, co i jak długo oglądają poszczególne osoby i uzyskać szczegółowy profil użytkownika, dostarczając wysoce dostosowane reklamy”.

„Funkcjonalność monitorowania została już wdrożona w aplikacjach mobilnych i może w najbliższej przyszłości stać się poważnym zagrożeniem dla prywatności” – dodali naukowcy.

Naukowcy z Braunschweig University of Technology odwiedzili dziesiątki sklepów w dwóch nienazwanych europejskich miastach i znaleźli cztery sklepy nadające te sygnały. Odnotowali również wzrost liczby aplikacji na Androida, które wyszukiwały te sygnały audio, z 39 w 2015 r. do 234 obecnie.

Ta technologia stała się punktem zainteresowania amerykańskiej Federalnej Komisji ds. Handlu, która w ubiegłym roku napisała do developerów aplikacji prosząc o wyjaśnienie, czy używali oprogramowania takiego jak Silverpush.

„Aplikacje te są w stanie słuchać w tle i zbierać informacje o konsumentach bez informowania ich” – powiedziała Jessica Rich, dyrektor Biura Ochrony Konsumentów FTC. „Firmy powinny informować ludzi, jakie informacje zbierają, jak je zbierają i z kim się nimi dzielą.”

Inteligentne urządzenia zdolne do szpiegowania obywateli nie są niczym nowym. Na początku bieżącego roku WikiLeaks wydało całą serię dokumentów CIA w ramach Vault 7, przedstawiając szczegółowo w jaki sposób agencja stworzyła złośliwe oprogramowanie o nazwie „Weeping Angel”, które zmienia inteligentne telewizory Samsung w urządzenia do podsłuchiwania, nawet jeśli urządzenie jest wyłączone.

„Weeping Angel może również wykraść loginy i hasła użytkowników oraz klucze Wi-Fi – umożliwiając dostęp do sieci i innych podłączonych urządzeń” – podał Mikael Thalen.

Autorstwo: Jamie White

Źródło oryginalne: Infowars.com

Źródło polskie: PrisonPlanet.pl