

Dane ze smartfonów można wykraść dzięki śledzeniu psów

8 grudnia 2021

Okazało się, że oprócz informacji o zwierzętach, czujniki aktywności psów współpracują z danymi osobowymi właścicieli na smartfonach i dlatego mogą zostać przechwycone przez cyberprzestępców. Obecnie lokalizatory GPS są aktywnie wykorzystywane przez właścicieli psów do stałego monitorowania swoich zwierząt. Zwykle takie urządzenie wygląda jak obroża z czujnikiem, który umożliwia ustalenie położenia zwierzaka i śledzenie jego cech fizjologicznych. Wyniki badań zostały opublikowane w czasopiśmie „International Journal of Computer Science”.

W takim przypadku czujniki wymieniają informacje z gadżetami właścicieli, które zawierają dane osobowe. Do tej pory temat zagrożeń dla danych osobowych występujących w tych systemach był mało zbadany. „Przeanalizowaliśmy podatność urządzeń monitorujących na cyberataki za pośrednictwem kanałów stron trzecich. Ten rodzaj ataku zbiera i wykorzystuje informacje uzyskane z fizycznych elementów systemu, na przykład szybkość obliczeń, sygnały elektromagnetyczne, akustyczne i wiele innych. W bieżącym badaniu symulowaliśmy cyberataki za pomocą sygnału elektromagnetycznego” – wyjaśnia Alla Levina, profesor nadzwyczajny Departamentu Bezpieczeństwa Informacji ETU „LETI”.

Naukowcy odkryli, że producenci urządzeń śledzących psy nie zwracają wystarczającej uwagi na bezpieczeństwo informacji urządzeń, z tego powodu atakujący mają możliwość uzyskania wszelkich poufnych danych, jakie kiedykolwiek trafiły do urządzenia śledzącego ze smartfona właściciela zwierzęcia. „Najbardziej niebezpieczną rzeczą jest to, że przestępcy mają możliwość połączenia się z telefonem właściciela psa za pomocą takiego urządzenia śledzącego. W praktyce jeszcze nie

przeprowadziliśmy takiego ataku, ale teoretycznie są do tego wszystkie przesłanki” – dodaje Alla Levina.

Ilość informacji, które można uzyskać od lokalizatora za pomocą sygnału elektromagnetycznego, zależy od zasady działania urządzenia. Niektóre z lokalizatorów mogą żądać informacji zawierających dużą ilość danych osobowych właściciela. „Na podstawie wyników badania twórcy urządzeń śledzących otrzymują zestaw konkretnych zaleceń w zależności od zidentyfikowanych luk w zabezpieczeniach, wskazano „słabe punkty”, które atakujący mogą wykorzystać do uzyskania informacji”, wyjaśnia Dmitry Kaplun, inny uczestnik badań, profesor nadzwyczajny Zakład Automatyki i Kontroli Procesów w ETU „LETI”.

W przyszłości naukowcy planują zbadać inne rodzaje zagrożeń, które mogą wynikać ze strony właścicieli psów korzystających z urządzeń monitorujących.

Autorstwo: tallinn

Źródło: ZmianyNaZiemi.pl