**Samochodowe systemy multimedialnej rozrywki mogą zostać wykorzystane do kradzieży danych z Twojego telefonu**

**Instalowane w nowoczesnych samochodach multimedialne systemy rozrywki i łączności stają się coraz popularniejsze. Wykryte w nich luki bezpieczeństwa umożliwiają kradzież wrażliwych danych znajdujących się na sparowanym telefonie.**

Tego typu ataki nazywa się CarsBlues. Niedawno zaprezentowany przez Andreę Amico – twórcę aplikacji mobilnej Privacy4Cars – pozwala na nieautoryzowany dostęp, za pośrednictwem Bluetootha, do telefonu sparowanego z samochodowym systemem rozrywki i przechwycenie danych dotyczących historii połączeń, listy kontaktów oraz wiadomości SMS.

Problem został już zgłoszony do Sharing and Analysis Center (Auto-ISAC) – organizacji zrzeszającej producentów samochodów w celu wymiany informacji i szybkiego reagowania na cyberzagrożenia. Dwóch producentów samochodów zadeklarowało już wprowadzenie stosownych poprawek w modelach na rok 2019. Szacuje się jednak, że luka nadal jest obecna w milionach pojazdów.

Jest to już kolejna wykryta luka pozwalająca na przeprowadzenie ataku CarsBlues. W ubiegłym roku dwóch analityków bezpieczeństwa sieciowego, Gabriel Cirlig i Stefan Tanase z IXII Group Inc, zaprezentowało atak na samochodowy system multimedialny za pomocą spreparowanego kodu napisanego w języku skryptowym. Atak umożliwiał pozyskanie z podłączonego telefonu historii połączeń, listę kontaktów, wiadomości SMS, emaile oraz powiązane z zainstalowanymi aplikacjami zdjęcia i nagrania. Wykradzione dane były następnie bez wiedzy użytkownika kopiowane na podpięty do samochodu pendrive.

Do przeprowadzenia naruszeń zaprezentowanych zarówno przez duet Gabriel Cirlig i Stefan Tanase (za pośrednictwem WiFi), jak i Andreę Amico (za pośrednictwem Bluetooth) nie jest wymagana fizyczna ingerencja. Wystarczy tylko sparować wcześniej urządzenie znajdujące się w posiadaniu przestępcy z samochodowym systemem rozrywki lub podłączyć się do samochodowej sieci WiFi.

Privacy4Cars ostrzega, że problem dotyczy głównie osób korzystających z wynajętych pojazdów. Nigdy nie mamy pewności, czy ktoś wcześniej nie zmodyfikował znajdującego się w wynajętym samochodzie oprogramowania, np. w celu gromadzenia w jego pamięci wewnętrznej wrażliwych danych z parowanych telefonów komórkowych.

*Problem jest bardzo poważny. Opisane luki dotyczyły konkretnych modeli samochodów i zostały usunięte. Warto jednak mieć świadomość tego, że różni producenci, różnych marek, często korzystają z takich samych lub nieznacznie modyfikowanych bibliotek kodu, co zwiększa prawdopodobieństwo, że na rynku występuje jeszcze wiele podatnych na atak samochodowych systemów cyfrowej rozrywki i łączności,* komentuje Dariusz Woźniak, inżynier techniczny Bitdefender z firmy Marken.