

Firma McAfee opublikowała raport „Caution: Malware Ahead” („Uwaga: złośliwe oprogramowanie na drodze”) przygotowany we współpracy z firmami Wind River i ESCRYP. Jest to pierwszy tego typu raport dotyczący bezpieczeństwa systemów elektronicznych stosowanych w samochodach.

W nowoczesnych samochodach systemy elektroniczne są powszechnie wykorzystywane do sterowania niemal wszystkimi urządzeniami łącznie z poduszkami powietrznymi, radiem, elektryczną regulacją siedzeń, ABS-em, systemami kontroli trakcji, systemami automatycznego utrzymywania bezpiecznej odległości (Autonomous Cruise Control, ACC), a także z systemami łączności i łączności wewnętrznej.

Naukowcy z kilku uniwersytetów wykazali, że mając dostęp do elektronicznych elementów samochodu (z wnętrza samochodu lub zdalnie przez Bluetooth) można uzyskać dostęp również do elementów istotnych dla bezpieczeństwa jazdy i pasażerów. Wykazano także, że za pomocą zaawansowanych czytników dalekiego zasięgu możliwe jest śledzenie pojazdu i zagrożenie prywatności pasażerów poprzez namierzanie znaczników RFID (stosowanych w wielu samochodach np. do monitorowania ciśnienia w oponach) nawet z odległości kilkudziesięciu metrów.

“Ponieważ coraz więcej funkcji w samochodach jest realizowanych elektronicznie, wzrasta zagrożenie atakami i zakłócania pracy istotnych urządzeń” – powiedział Stuart McClure, wiceprezes i dyrektor generalny z firmy McAfee. „Przeprowadzone badania dowodzą istnienia rzeczywistego zagrożenia bezpieczeństwa konsumentów. Ryzyko włamania do poczty elektronicznej czy laptopa to jedno, ale włamanie do systemów elektroniki samochodowej może stanowić bardzo poważne zagrożenie bezpieczeństwa”.

Przemysł motoryzacyjny wciąż dodaje nowe funkcje i udogodnienia, takie jak dostęp do Internetu czy możliwość dostosowania wielu właściwości pojazdu do preferencji użytkownika. Ponadto użytkownicy chcą mieć stały dostęp do Internetu nawet podczas jazdy, a to skłania producentów do coraz głębszej integracji systemów elektroniki samochodowej z urządzeniami konsumenckimi, takimi jak smartfony czy tablety. Niestety, w tej sytuacji kwestie bezpieczeństwa spadają na drugi plan. W raporcie zaprezentowano m.in. przykłady włamań do systemów elektronicznych zainstalowanych w samochodach.

Raport firmy McAfee opisuje ryzyka związane z narażeniem na działania cyberprzestępców, takie jak:

- zdalne otwieranie i uruchamianie samochodu przy pomocy telefonu komórkowego
- zdalne zablokowanie samochodu
- śledzenie położenia samochodu i działań kierowcy
- kradzież danych osobowych poprzez Bluetooth
- zakłócanie nawigacji samochodowej
- zablokowanie systemu wzywania pomocy

“W branży motoryzacyjnej widoczna jest konwergencja elektroniki samochodowej i użytkowej. Konsumenti coraz częściej oczekują, że w pojazdach będą mieli możliwości i funkcje analogiczne do najnowszych gadżetów elektronicznych i urządzeń mobilnych. Jednak ze wzrostem powszechności dostępu do Internetu rośnie też ryzyko włamania na skutek wykorzystania słabości systemów samochodowych” – powiedział Georg Doll, dyrektor ds. rozwiązań motoryzacyjnych w firmie Wind River. „Raport zwraca uwagę na rzeczywiste obawy związane z bezpieczeństwem, a wiele firm z branży motoryzacyjnej już pracuje nad rozwiązaniem tych problemów. Jednak biorąc pod uwagę długość cyklu projektowania samochodów konieczna jest ścisła współpraca ze specjalistami od oprogramowania”.

Pełen raport dostępny jest na stronie: [www.mcafee.com/autoreport](http://www.mcafee.com/autoreport).

**McAfee**