Motoryzacyjna ruletka

ID artykułu: 58062 / 2264

URL: http://www.publikuj.org/58062

Badacze z firmy Kaspersky przeanalizowali nieoryginalne urządzenia dla samochodów, dzięki którym można przekształcić je w inteligentne pojazdy. Ta nisza okazała się bezpieczniejsza niż akcesoria Internetu Rzeczy. Samochód połączony z internetem można obecnie uzyskać na dwa sposoby zakupić u dealera gotowy inteligentny pojazd lub udoskonalić posiadane auto za pomocą kilku dodatkowych inteligentnych urządzeń. Obie metody pozwalają osiągnąć większy komfort jazdy, trzeba jednak pamiętać, że omawiana technologia to nowy obszar, który daje ogromne pole do popisu cyberprzestępcom, co zostało potwierdzone zarówno w doniesieniach medialnych, jak i badaniach firmy Kaspersky. Jest to naturalna kolej rzeczy gdy jakaś technologia staje się popularna, wzrasta liczba związanych z nią incydentów dotyczących bezpieczeństwa.

W związku z tym badacze z firmy Kaspersky postanowili zbadać, czy tego rodzaju doniesienia dotyczące bezpieczeństwa urządzeń Internetu Rzeczy mają jakikolwiek wpływ na producentów inteligentnych urządzeń dla branży motoryzacyjnej. W tym celu przeanalizowano kilka losowo wybranych urządzeń, w tym zewnętrzne narzędzie skanujące podłączane pod port OBD pojazdu, system monitorowania ciśnienia i temperatury opon, inteligentny system alarmowy, urządzenie śledzące GPS oraz kamerę samochodową sterowaną za pomocą aplikacji.

Wyniki stanowiły miłe zaskoczenie: chociaż branża Internetu Rzeczy często uważana jest za podatną na zagrożenia, badane inteligentne urządzenia przeznaczone dla samochodów okazały się dość bezpieczne, nie wykazując poważniejszych luk w zabezpieczeniach. Niemniej jednak zidentyfikowano kilka problemów dotyczących bezpieczeństwa: możliwość uzyskania zdalnego dostępu do danych dot. dynamiki jazdy za pośrednictwem narzędzia skanującego, możliwość manipulowania sygnałami z systemu monitorowania ciśnienia w oponach oraz możliwość otworzenia drzwi pojazdu przy użyciu systemu alarmowego. Na szczęście wszystkie te działania są bardzo trudne do realizacji lub nie przynoszą przestępcy żadnych oczywistych ani natychmiastowych efektów.

Zbadane przez nas urządzenia spełniały wymogi wielu zasad bezpieczeństwa i z wyjątkiem kilku drobnych problemów zostały uznane za zadowalające pod tym względem. Wynika to częściowo z faktu, że produkty te posiadają ograniczoną funkcjonalność, a przeprowadzenie ataku za ich pośrednictwem nie spowoduje poważnych konsekwencji. Z drugiej strony jest to również zasługa dbałości producentów. Cieszymy się, że zatroszczyli się o zabezpieczenie swoich urządzeń jest to dobry znak dla branży motoryzacyjnej. Mimo to nie należy spoczywać na laurach: z naszego doświadczenia wynika, że im bardziej inteligentne urządzenie, tym większe prawdopodobieństwo wystąpienia problemów związanych z bezpieczeństwem. Kwestie bezpieczeństwa powinno się uwzględniać już na początkowych etapach rozwoju produktu, szczególnie gdy na rynek wchodzi nowa generacja inteligentnych urządzeń powiedział Wiktor Czebyszew, ekspert ds. cyberbezpieczeństwa z firmy Kaspersky.

Porady bezpieczeństwa W celu zapewnienia większego bezpieczeństwa inteligentnym urządzeniom samochodowym eksperci z firmy Kaspersky zalecają następujące działania:

Wybierając element pojazdu, który ma być nieco bardziej inteligentny, rozważ najpierw zagrożenia związane z bezpieczeństwem. Bądź szczególnie czujny, gdy urządzenie ma coś wspólnego z telemetrią pojazdu lub dostępem do systemów odpowiadających za bezpieczeństwo czynne i bierne. Zanim kupisz urządzenie, przeszukaj internet pod kątem informacji o jakichkolwiek lukach w jego zabezpieczeniach. Być może urządzenie, które chcesz nabyć, zostało już sprawdzone przez badaczy i dowiesz się, jakie problemy zostały w nim wykryte bądź usunięte. Produkty, które zostały niedawno wprowadzone na rynek, nie zawsze są najlepszym wyborem. Oprócz standardowych błędów, które są często identyfikowane w nowych produktach, najnowsze modele urządzeń mogą zawierać problemy związane z bezpieczeństwem, które nie zostały jeszcze wykryte przez badaczy bezpieczeństwa. Najlepiej zdecydować się na produkt, dla którego opublikowano już

kilka aktualizacji oprogramowania. Zawsze rozważ bezpieczeństwo mobilnego aspektu urządzenia, szczególnie gdy posiadasz urządzenia z systemem Android aplikacje często są przydatne i ułatwiają życie, jednak infekcja smartfona szkodliwym oprogramowaniem może mieć poważne skutki. W celu sprostania wyzwaniu związanym z cyberbezpieczeństwem inteligentnych urządzeń firma Kaspersky rozwinęła system KasperskyOS, który jest wykorzystywany w sprzęcie i oprogramowaniu. System ten może być stosowany w urządzeniach przenośnych oraz komputerach stacjonarnych, urządzeniach Internetu Rzeczy, inteligentnych systemach energetycznych, systemach przemysłowych, telekomunikacji oraz systemach transportowych. Firma Kaspersky dostrzega potencjał w dalszym rozwoju systemu KasperskyOS w zakresie spełnienia potrzeb swoich klientów oraz zapewnienia najwyższego poziomu bezpieczeństwa we wszystkich tych obszarach, łącznie z branżą motoryzacyjną. Więcej informacji na ten temat znajduje się na stronie https://os.kaspersky.com.

Szczegóły techniczne dotyczące badania wykorzystanego w niniejszej informacji prasowej są dostępne na stronie https://r.kaspersky.pl/qs65Z.

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Kaspersky jako źródła.

Wszystkie informacje prasowe są dostępne na stronie https://www.kaspersky.pl/nowosci.

Piotr Kupczyk
Dyrektor biura komunikacji z mediami, Kaspersky Lab Polska
E-mail: piotr.kup czyk@kaspersky.pl
Tel. 34 390 94 00

Aktywacja: 22/07/19 13:22, odsłony: 79