

Chińskie pojazdy elektryczne mogą stać się zdalnie sterowaną bronią w wojnie hybrydowej



- Chińskie pojazdy elektryczne stanowią poważne zagrożenie dla cyberbezpieczeństwa dzięki wbudowanym funkcjom nadzoru i zdalnego uzbrojenia.
- Eksperci ds. cyberbezpieczeństwa ostrzegają, że pojazdy te mogą zostać przejęte w celu wyłączenia funkcji bezpieczeństwa, wywołania eksplozji lub sparaliżowania miast podczas konfliktów.
- W samym tylko sierpniu w Australii sprzedano ponad 20 000 chińskich pojazdów elektrycznych wyposażonych w ryzykowne moduły komórkowego internetu rzeczy (CIM).
- Wzywa się rządy do zakazania chińskim producentom pojazdów elektrycznych udziału w przetargach publicznych, chyba że zezwolą oni na kontrolę kodu źródłowego i audyt danych.
- Kraje zachodnie stoją w obliczu rosnącego ryzyka, ponieważ 80% pojazdów elektrycznych w Australii jest obecnie produkowanych w Chinach, a podobne trendy pojawiają się na całym świecie.

Wyobraź sobie, że jedziesz ruchliwą autostradą, gdy nagle bateria Twojego pojazdu elektrycznego przegrzewa się – lub, co

gorsza, eksploduje. Teraz wyobraź sobie, że dzieje się to jednocześnie z tysiącami samochodów, paraliżując ruch, powodując masowe ofiary śmiertelne i pogrążając miasta w chaosie.

Nie jest to fabuła dystopijnego thrillera, ale bardzo realne zagrożenie stwarzane przez pojazdy elektryczne produkowane w Chinach, według eksperta ds. cyberbezpieczeństwa Alastaira MacGibbona.

Podczas tegorocznego szczytu Australian Financial Review Cyber Summit MacGibbon, były doradca premiera Malcolma Turnbulla ds. cyberbezpieczeństwa, wydał mrożące krew w żyłach ostrzeżenie: chińskie pojazdy elektryczne eksploatowane w Australii mogą zostać zdalnie wykorzystane jako broń w ramach kampanii wojny hybrydowej. Wyjaśnił, że pojazdy te nie służą wyłącznie do transportu; są to [urządzenia monitorujące z wbudowanymi wyłącznikami awaryjnymi](#), które mogą zostać przejęte przez zagranicznych przeciwników w celu wyłączenia funkcji bezpieczeństwa, wywołania eksplozji, a nawet sparaliżowania całego miasta w godzinach szczytu.

MacGibbon, obecnie dyrektor ds. strategii w CyberCX, nie przebierał w słowach. „Samochody, o których mówimy, niezależnie od tego, czy są elektryczne, czy nie, są urządzeniami podsłuchowymi i urządzeniami monitorującymi w postaci kamer” – stwierdził. Jednak zagrożenia wykraczają daleko poza naruszenie prywatności. „Wystarczy wyłączyć funkcje bezpieczeństwa domowych akumulatorów, aby się przeładowały. Wystarczy wyłączyć te same funkcje bezpieczeństwa w pojazdach elektrycznych. Wystarczy wyłączyć je u producenta, aby pojazdy te eksplodowały. Wystarczy ograniczyć ich zdolność do poruszania się w godzinach szczytu w wybranych miastach”.

Jego ostrzeżenia są zgodne z coraz większą liczbą dowodów sugerujących, że chińska strategia „wojny totalnej” wykorzystuje podłączone do sieci urządzenia jako broń. Od

handlu fentanylem po stosowanie broni biologicznej – Komunistyczna Partia Chin (KPCh) wykazała gotowość do wykorzystywania słabości technologicznych w celu destabilizacji przeciwników. Obecnie, gdy cztery chińskie marki pojazdów elektrycznych – BYD, GWM, MG Motor i Chery – po raz pierwszy znalazły się w pierwszej dziesiątce najlepiej sprzedających się marek w Australii, ryzyko to nie jest już tylko teoretyczne. Dziesiątki tysięcy tych pojazdów jeździ już po australijskich drogach, wyposażonych w moduły komórkowego internetu rzeczy (CIM), które przesyłają dane do chińskich serwerów.

Trojan na kołach?

[Zagrożenie](#) nie jest tylko hipotetyczne. Tylko w sierpniu Australijczycy kupili ponad 20 000 pojazdów wyprodukowanych w Chinach, a BYD wyprzedził Mitsubishi, stając się szóstą najlepiej sprzedającą się marką samochodów w kraju. Pojazdy te są wyposażone w moduły CIM, niewielkie, ale potężne urządzenia, które umożliwiają zdalne aktualizacje oprogramowania, udostępnianie danych o ruchu drogowym, a nawet śledzenie lokalizacji w czasie rzeczywistym. Według raportu China Strategic Risks Institute (CSRI) moduły te tworzą tylne drzwi dla cyberataków, umożliwiając Pekinowi unieruchomienie pojazdów, zbieranie poufnych danych, a nawet sabotowanie krytycznej infrastruktury w przypadku konfliktu.

Chiny mogłyby zdalnie unieruchomić floty pojazdów elektrycznych, unieruchamiając kierowców, zakłócając działanie służb ratowniczych lub nawet gorzej. Think tank zaleca, aby rządy zakazały chińskim producentom pojazdów elektrycznych udziału w przetargach publicznych, chyba że poddadzą się kontroli kodu źródłowego i regularnym audytom swoich globalnych centrów danych – co jest żądaniem, którego Pekin prawdopodobnie nie spełni.

Ostrzeżenia MacGibbona wykraczają poza pojazdy elektryczne.

„Potencjalnie miliony urządzeń [Internetu rzeczy] lub urządzeń podłączonych do sieci – nie wyprodukowanych w Chinach, ale kontrolowanych przez Chiny – znajdują się w naszych systemach” – zauważył. Obejmuje to panele słoneczne, domowe akumulatory, a nawet dachowe podgrzewacze słoneczne, z których wiele zostało już oznaczonych jako podejrzane ze względu na wbudowaną technologię.

Czas się obudzić

Australia nie jest jedynym krajem, który bije na alarm. Stany Zjednoczone zaproponowały zakaz importu chińskich pojazdów elektrycznych z powodu podobnych obaw, a brytyjscy urzędnicy są naciskani, aby zobowiązać zagranicznych dostawców do nieprzekazywania danych w żadnych okolicznościach.

Jednak pomimo ostrzeżeń chińskie pojazdy elektryczne nadal zalewają rynki zachodnie dzięki niskim cenom i agresywnemu marketingowi. Ponieważ 80% pojazdów elektrycznych w Australii jest obecnie produkowanych w Chinach, pytanie nie brzmi, czy pojazdy te mogą zostać wykorzystane jako broń, ale kiedy i jak poważne będą tego skutki.

Konsekwencje są ogromne. W scenariuszu wojny hybrydowej Pekin nie musiałby wystrzelić ani jednej rakiety, aby sparaliżować miasto. Kilka linii złośliwego kodu mogłoby unieruchomić hamulce, wywołać pożary lub zamienić tysiące samochodów w blokady dróg, wywołując masową panikę i szkody gospodarcze.

Chińskie pojazdy elektryczne to nie tylko samochody – to potencjalna broń. Jeśli rządy zachodnie nie podejmą natychmiastowych działań, wkrótce mogą znaleźć się w sytuacji, w której zostaną przechytrzone przez konia trojańskiego na kołach.