tom's HARDWARE

Producent wydaje polecenie zdalnego wyłączenia inteligentnego odkurzacza po tym, jak inżynier zablokował mu możliwość zbierania danych — użytkownik przywraca go do działania za pomocą niestandardowego sprzętu i skryptów Pythona, aby działał w trybie offline

Autor Jowi Morales opublikowano 1 listopada 2025 r.

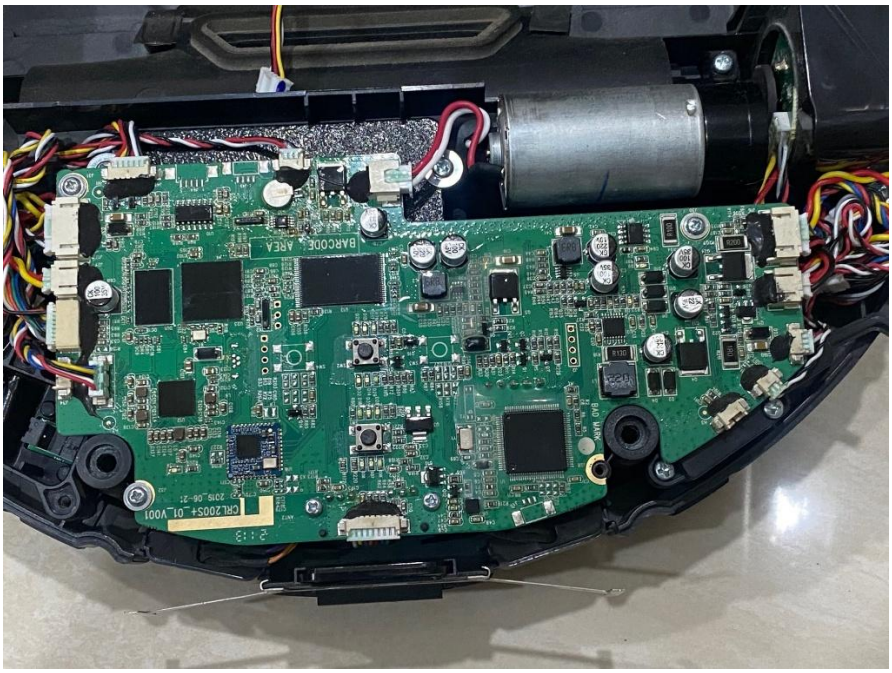
Inteligentny odkurzacz został zdalnie uszkodzony, ponieważ nie zbierał danych.

(Źródło obrazu: Getty Images)

Inżynier zainteresował się działaniem swojego inteligentnego odkurzacza iLife A11 i monitorował ruch sieciowy pochodzący z urządzenia. Zauważył wtedy, że urządzenie stale wysyła logi i dane telemetryczne do producenta – na co nie wyraził zgody. Użytkownik, Harishankar, postanowił zablokować adresy IP serwerów telemetrycznych w swojej sieci, jednocześnie pozostawiając otwarte oprogramowanie sprzętowe i serwery OTA. Chociaż jego inteligentny gadżet działał przez jakiś czas, wkrótce potem po prostu odmówił uruchomienia. Po długim dochodzeniu odkrył, że do jego urządzenia wydano polecenie zdalnego wyłączenia.

Kilkakrotnie wysyłał go do serwisu, gdzie technicy włączali go i nie widzieli żadnych usterek. Po zwróceniu działał przez kilka dni, a potem znowu się nie uruchamiał. Po kilku próbach serwis prawdopodobnie zmęczył się i po prostu przestał go przyjmować, twierdząc, że gwarancja wygasła. Z tego powodu postanowił rozebrać urządzenie, aby ustalić, co je uszkodziło i sprawdzić, czy uda mu się je ponownie uruchomić.

Ponieważ A11 był urządzeniem inteligentnym, posiadał układ SoC AllWinner A33 z systemem operacyjnym TinaLinux oraz mikrokontroler GD32F103 do zarządzania mnóstwem czujników, w tym lidarem, żyroskopami i enkoderami. Stworzył złącza PCB i napisał skrypty w Pythonie, aby sterować nimi za pomocą komputera, prawdopodobnie po to, aby przetestować każdy element osobno i zidentyfikować przyczynę usterki. Następnie zbudował joystick Raspberry Pi do ręcznego sterowania odkurzaczem, udowadniając, że sprzęt działa prawidłowo.

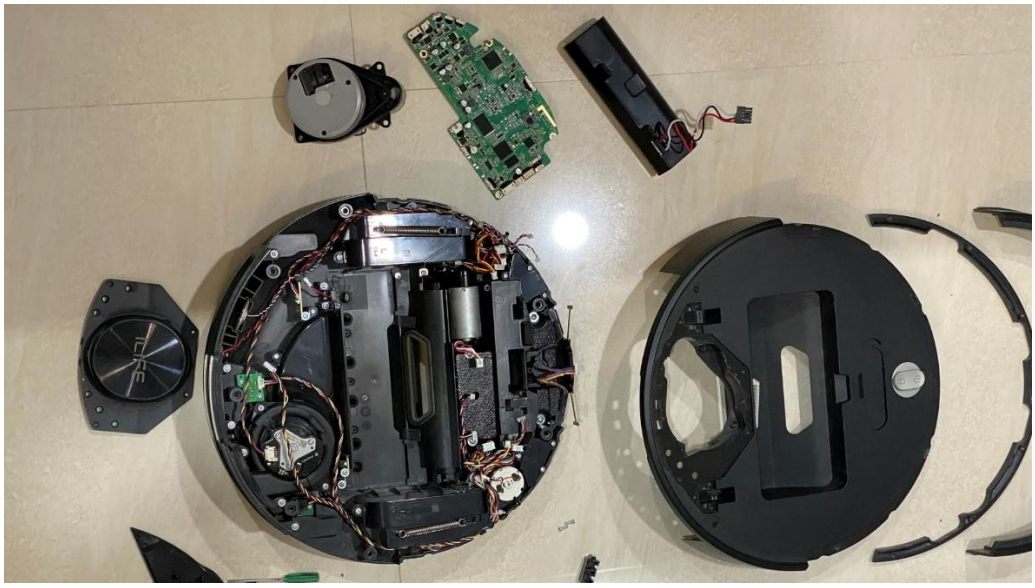


(Źródło obrazu: Harishankar)

Następnie przyjrzał się oprogramowaniu i systemowi operacyjnemu i tam odkrył mroczną prawdę: jego inteligentny odkurzacz był koszmarem bezpieczeństwa i czarną dziurą dla jego danych osobowych. Po pierwsze, Android Debug Bridge, dający mu pełny dostęp root do odkurzacza, nie był chroniony żadnym hasłem ani szyfrowaniem. Producent dodał prowizoryczny protokół bezpieczeństwa, pomijając kluczowy plik, co spowodowało rozłączenie wkrótce po uruchomieniu, ale Harishankar z łatwością go ominął. Następnie odkrył, że odkurzacz używał Google Cartographer do tworzenia trójwymiarowej mapy jego domu na żywo.

To zdecydowanie nic niezwykłego. W końcu to inteligentny odkurzacz i potrzebuje tych danych, aby poruszać się po jego domu. Niepokojące jest jednak to, że wysyłał wszystkie te dane na serwer producenta. To logiczne, że urządzenie wysyła te dane do producenta, ponieważ jego wbudowany układ SoC nie jest wystarczająco wydajny, aby przetworzyć wszystkie te dane. Wygląda jednak na to, że iLife nie wyjaśniło tego swoim klientom. Co więcej, inżynier dokonał

niepokojącego odkrycia – głęboko w logach swojego niedziałającego inteligentnego odkurzacza znalazł polecenie z sygnaturą czasową, która dokładnie odpowiadała czasowi, w którym gadżet przestał działać. Było to ewidentnie polecenie wyłączające, a po jego cofnięciu i ponownym uruchomieniu urządzenie z rykiem powróciło do życia.



(Źródło obrazu: Harishankar)

Dlaczego więc A11 działał w centrum serwisowym, ale odmówił uruchomienia w domu? Technicy resetowali oprogramowanie układowe inteligentnego odkurzacza, usuwając w ten sposób kod zabezpieczający, a następnie podłączali go do otwartej sieci, co pozwalało mu działać normalnie. Jednak po ponownym połączeniu z siecią, której serwery telemetryczne były zablokowane, urządzenie zostało zdalnie uszkodzone, ponieważ nie mogło komunikować się z serwerami producenta. Ponieważ zablokował on możliwości gromadzenia danych przez urządzenie, producent postanowił je po prostu całkowicie wyłączyć. „Ktoś – lub coś – zdalnie wydał polecenie wyłączenia” – mówi Harishankar. „Niezależnie od tego, czy była to celowa kara, czy automatyczne egzekwowanie „zgodności”, rezultat był ten sam: urządzenie konsumenckie wyłączyło się”.

Niestety, wiele innych marek inteligentnych odkurzaczy korzysta z podobnego sprzętu, więc nie jest wykluczone, że mają taką samą konfigurację. Dotyczy to szczególnie tańszych urządzeń, które mają mniej wydajny sprzęt i nie obsługują przetwarzania brzegowego, co oznacza, że będą musiały przesłać dane do jakiegoś odległego serwera w celu przetworzenia. Ponieważ jednak Twoje dane są przesyłane na inne urządzenie poza Twoją kontrolą, tak naprawdę nie masz pojęcia, co się z nimi dzieje, dając producentowi pełną swobodę w ich wykorzystaniu.

W końcu, po wszystkich wprowadzonych modyfikacjach, właściciel mógł uruchomić swój odkurzacz w pełni lokalnie, bez kontroli producenta. To pomogło mu odzyskać kontrolę nad swoimi danymi i korzystać z jego wartego 300 dolarów, uszkodzonego oprogramowania, na własnych warunkach. A dla nas, którzy nie mamy wiedzy technicznej i czasu, aby śledzić jego osiągnięcia, jego rada brzmi: „Nigdy nie korzystaj z głównej sieci Wi-Fi dla urządzeń IoT” i „traktuj je jak obce osoby w domu”.