Śmierć z laptopa

18 października 2012

Znany ekspert ds. bezpieczeństwa, Barnaby Jack, twierdzi, że cyberprzestepca może zabić osobę z wszczepionym rozrusznikiem serca. Śmiertelny atak można przeprowadzić za pomocą laptopa znajdującego się w odległości nawet ponad 40 metrów od ofiary.

Barnaby Jack, który przemawiał podczas australijskiej konferencji Breakpoint, ostrzega, że wskutek błędów programistycznych w bezprzewodowych przekaźnikach możliwe jest zdalne zaaplikowanie impulsu o napięciu 830 woltów.

Ekspert poinformował, że w samych tylko Stanach Zjednoczonych w latach 2006-2011 sprzedano 4,6 miliona rozruszników i wszczepialnych kardiowerterów-defibrylatorów. W przeszłości urządzenia te mogły być przeprogramowane pod warunkiem, że w odległości nie większej niż kilku metrów od pacjenta użyto specjalnego przełącznika, dającego dostęp do oprogramowania. Jednak wraz z rozwojem technologii coraz więcej producentów stosuje rozwiązania bezprzewodowe, pozwalające na przeprogramowanie z odległości kilkudziesięciu metrów bez potrzeby używania wcześniej wykorzystywanego „przełącznika”. Przed sześcioma laty FDA zezwoliła na używanie w implantach urządzeń radiowych pracujących na częstotliwości 400 MHz.

Barnaby Jack uważa, że taka zmiana podejścia ułatwia ataki. Ekspert zauważył, że za pomocą odpowiedniej komendy można zapytać urządzenie o jego numer serii i numer konkretnego urządzenia. Posiadając takie informacje możliwe jest przeprogramowanie nadajnika wbudowanego w implant tak, by pozwalał na zmianę ustawień samego rozrusznika czy defibrylatora. Barnaby zauważa, że FDA sprawdza tylko medyczną przydatność urządzenia, nie bada natomiast kodu źródłowego użytego oprogramowania.

Poza błędami, które mogą skończyć się śmiertelnym atakiem na

pacjenta, Barnaby Jack znalazł również inne niedociągnięcia w oprogramowaniu implantów. Odkryte dziury pozwalają np. uzyskać dostęp do danych pacjenta i jego lekarza czy też włamać się do serwerów wykorzystywanych przez osoby tworzące oprogramowanie dla implantów.

Obecnie ekspert pracuje nad aplikacją „Electric Feel", która będzie wyposażona w graficzny interfejs użytkownika i pozwoli na odszukiwanie znajdujących się w pobliżu implantów oraz wydanie im polecenia zaprzestania pracy lub dostarczenia wyładowania o zadanej mocy. To jednak nie koniec. Barnaby Jack twierdzi, że możliwe jest zarażenie serwerów wykorzystywanych przez programistów i spowodowanie by szkodliwy kod, za ich pośrednictwem, trafił do implantów tysięcy osób. „Możemy w ten sposób stworzyć robaka zdolnego do popełnienia masowego morderstwa – mówi badacz.

Zadziwiać może fakt, że badane przez Jacka urządzenia są wyposażone w szyfrowanie AES, ale nie jest ono włączone. Ponadto zawierają tylne drzwi, które pozwalają programistom na dostęp do urządzenia bez przechodzenia standardowego procesu weryfikacji.

Opracowanie: Mariusz Błoński
Na podstawie: Computerworld
Źródło: Kopalnia Wiedzy