Intel rozwija system zdalnego blokowania laptopów

25 czerwca 2014

Intel opracowuje system zdalnego blokowania laptopów „Kill Switch", który umożliwia zdalne monitorowanie i wyłączanie urządzeń, co jest niepokojącą perspektywą patrząc na związek tego przedsiębiorstwa z Agencją Bezpieczeństwa Narodowego NSA.

„Gigant produkujący chipy pracuje z wieloma partnerami nad czymś co nazywa się Wireless Credential Exchange (WCE). Jego chipy będą komunikować się z chipami Impinj's Monza RFID aby umożliwić zdalne monitorowanie urządzeń za pomocą oprogramowania Burnside Digital IPTrak" pisze Sean Portnoy z gazety ZD Net. „Oznaczałoby to, że urządzenia te mogą być kontrolowane tak by włączyły się tylko wtedy, gdy dotrą do zatwierdzonego miejsca przeznaczenia lub w określoną lokalizację. Jeśli nie dotrą na miejsce przeznaczenia lub nie opuszczą zatwierdzonego obszaru, to mogą być wyłączone."

Technologia ta sprzedawana jest jako sposób na powstrzymanie kradzieży, ale może powodować prawdziwą konsternację wśród zwolenników prywatności.

Jak pisaliśmy we wrześniu, bardziej prymitywna wersja „Kill Switch" była faktycznie dodana do procesorów Intela w 2011 roku wraz z uruchomieniem antykradzieżowej platformy Anti Theft 3.0. Technologia ta umożliwiła Intelowi podsłuchiwanie aktywności komputera poprzez chip radiowy 3G, który może ominąć szyfrowanie twardego dysku. „Obejmują one komunikację poza standardowymi zakresami (łączność, która istnieje poza zakresem działania maszyny poprzez system operacyjny lub supervisora), monitoring i przerabianie przychodzącego i wychodzącego ruchu sieciowego", donosi TG Daily. „Krótko mówiąc, działa skrycie i podsłuchuje oraz potencjalnie manipuluje danymi."

W posnowdenowej erze, idea firm mających zdalny dostęp do komputera użytkownika oznacza potencjalne otwarcie puszki pandory dla naruszeń prywatności.

Jest powszechnie uznawanym faktem wśród ekspertów, że NSA „ma tajne systemy dostępu na poziomie sprzętu, wbudowane w procesory Intel i AMD.” Na początku tego roku w trakcie Reddit czatu online, szef Intela Brian Krzanich odmówił odpowiedzi na pytanie dotyczące tego, czy NSA ma możliwość tajnego dostępu.

W grudniu ubiegłego roku, twórcy systemu operacyjnego FreeBSD powiedzieli, że nie mogą już dłużej ufać systemom kryptograficznym opartym o chip Intela oraz VIA, ostrzegając, że istnieje duże prawdopodobieństwo, że NSA ma do nich tajny dostęp.

Pomysł firm mających dostęp do „Kill Switch” bez możliwości rezygnacji z takiej opcji przez osoby prywatne odbiera wolność jednostkom, pozostawiając otwarte drzwi dla rządów, które będą wykorzystywały tą technologię przeciw dysydentom, w podobny sposób jak niedawno zrobił to rząd Turcji zamykając Twittera by blokować skandal polityczny ze swoim udziałem.

Jak pisaliśmy w zeszłym tygodniu, wszystkie nowe telefony Android i Windows będą również wyposażone w „Kill Switch” w imię ochrony przed kradzieżą.

Zarówno firma Google jak i Apple złożyły patenty skupiające się na zdalnym wyłączaniu urządzeń, w sytuacjach gdy zdjęcia wykonywane są w obszarach wrażliwych dla organów ścigania lub na koncertach, tworząc technologiczne „martwe strefy”, co może być wykorzystywane do zakłócenia politycznych demonstracji lub wykolejania niechcianych serwisów informacyjnych.

Autor: Paul Joseph Watson
Źródło oryginalne: PrisonPlanet.com
Źródło polskie: PrisonPlanet.pl