Cyberdefence 24

**aut. Tomasz Fastyn** 21.07.2016

# LUDZIE MOGĄ STAĆ SIĘ NIEDŁUGO NOSICIELAMI WIRUSÓW… KOMPUTEROWYCH

W 2010 roku Mark Gasson nazywany przez media pierwszym człowiekiem zarażonym przez wirus komputerowy przestrzegał przed niewystarczającym skupianiu się nad kwestią cyberbezpieczeństwa nowo rozwijanych technologii. Dziś te słowa wydają się prorocze, implanty stosowane w odczytywaniu fal mózgowych posiadają dostęp do sieci Wi-Fi.

Pierwszy przypadek obecności wirusa komputerowego w chipie odnotowany został w ciele  Marka Gassona.  Chip, został wszczepiony w jego lewą rękę. Urządzenie przypomina te stosowane w celu identyfikacji zwierząt domowych. Sam Gasson wykorzystał chip jako kartę dostępową na teren kampusu Uniwersytetu Reading w Wielkiej Brytanii, jednocześnie tak zmodyfikował oprogramowanie swojego telefonu, aby działał tylko wtedy kiedy on z niego korzysta. Rok po wszczepieniu sobie chipa w 2010 roku, spostrzegł, że został zarażony wirusem komputerowym, który mógł dostać się do sieci komputerowej. Dodatkowo Mark Gasson ostrzegał już w 2010 przed problemami jakie mogą czekać przyszłe implanty czy urządzenia mobilne z w powodu niewystarczających mechanizmów cyberbezpieczeństwa jakie są stosowane w medycynie czy urządzeniach codziennego użytku.

– Nie możemy wykluczyć sytuacji, w której oprogramowanie ransomware uniemożliwi korzystanie z protezy ręki lub nogi, bądź zagrozi wyłączeniem rozrusznika serca. Jeśli spojrzeć na obecny poziom rozwoju technologii i pomysłowość hakerów, może to być bliższe rzeczywistości niż nam się wydaje – mówi ekspert z firmy Fortinet David Maciejak.

Infekcje oprogramowaniem ransomware już dziś są prawdziwą plagą, a ten stan może jeszcze ulec pogorszeniu. Wciąż istnieje jedna domena, która dotychczas pozostawała nietknięta przez to złośliwe oprogramowanie.

Według ekspertów są to przemysłowe systemy sterowania (ICS), oprogramowanie tej klasy jest wykorzystywane w zakładach chemicznych czy nawet elektrowniach atomowych. Opinii publicznej nie są znane jeszcze żadne ataki za pomocą ransomware w ten sektor. Jednak obecność takich wirusów jak Stuxnet w sieciach zarządzających pracą czy w ostatnim czasie obecność wirusa w komputerach elektrowni atomowej w Gundermmingen w Niemczech. W przypadku tego ostatniego procesy odpowiedzialne za prace samej elektrowni atomowej były przeprowadzane za pomocą analogowego systemu. Zazwyczaj takie sieci są odseparowane od dostępu do globalnej sieci, jednak nie trudno sobie wyobrazić scenariusz w którym ktoś przyniesie nawet niechcący zainfekowaną kartę SD czy klucz USB i podłączy go do bezpiecznej odseparowanej sieci.

Również w Stanach Zjednoczonych atakom ulga infrastruktura krytyczna. W 2013 r. przeprowadzono atak rozpoznawczy na tamę Bowman Avenue Dam w Nowym Jorku. Firma Calpine, największy amerykański producent energii elektrycznej z gazu ziemnego i źródeł geotermalnych, padła z kolei ofiarą kradzieży szczegółowych rysunków technicznych swojej infrastruktury.

Już istniejące oprogramowanie ransomware jest zdolne przeprowadzić tego typu atak — wystarczy, aby został on skierowany we właściwe miejsce. Całkiem realne wydaje się więc przeprowadzenie w najbliższych miesiącach ataku na obiekty, które mogą stanowić niezwykle dochodowy cel dla twórców ransomware. Wystarczy wyobrazić sobie, ile rządy byłyby w stanie zapłacić za uniknięcie konsekwencji ataku na elektrownię jądrową – podkreśla David Maciejak z Fortinet.

Problem będzie z obecnością ransomware na rynku złośliwego oprogramowanie będzie według Maciejaka narastał z każdym okupem zapłaconym przez osoby, których urządzenia zostały zaatakowane przez ten typ wirusa. Model biznesowy twórców oprogramowania ransomware przypomina ten znany z dużych korporacji, autorzy przeznaczają bowiem znaczą część pozyskanych środków na rozwój i badania – podkreśla.

Czytaj też: W systemach elektrowni atomowej w Niemczech znaleziono wirusa