Stuxneta stworzyły USA i Izrael

2 czerwca 2012

Stuxnet rzeczywiście był cyberbronią, którą stworzyły USA z Izraelem. Ta cyberbroń wydostała się na wolność, co nie było planowane – takie informacje podaje „New York Times" i nie stawiają one USA w dobrym świetle. Teraz Chiny i inne kraje, którym zarzucano cyberataki, będą mówić: „wy też to robicie".

W roku 2010 specjaliści firmy Kaspersky Lab przekazali światu sensacyjną informację – robak o nazwie Stuxnet był prawdopodobnie cyberbronią, stworzoną przez wojskowych specjalistów, która miała atakować elektrownię atomową w Iranie. Świadczył o tym jego bardzo wyrafinowany charakter, a także ukierunkowanie na specyficzne cele.

Natomiast „New York Times" potwierdza najważniejsze elementy tych informacji. Stuxnet miał być wspólnym dziełem USA oraz Izraela i miał służyć powstrzymaniu nuklearnych planów Iranu. Operacja była określana kryptonimem „Olympic Games". Wszystko zaczęło się jeszcze za kadencji Busha, ale obecny prezydent USA Barack Obama podjął decyzję o kontynuowaniu ataku, po tym jak wirus „wymknął się" na wolność.

Informacje na ten temat pochodzą z tekstu z „New York Times" pt. „Obama Order Sped Up Wave of Cyberattacks Against Iran", autorstwa Davida E. Sangera. Tekst jest opracowany na podstawie książki, która ma się niebawem ukazać („Confront and Conceal: Obama's Secret Wars and Surprising Use of American Power"). Informacje podawane przez Sangera zostały zebrane w serii wywiadów z amerykańskimi, europejskimi oraz izraelskimi urzędnikami, którzy oczywiście chcieli zachować anonimowość.

W chwili obecnej nie wiadomo, czy Iran faktycznie buduje bombę atomową. Nie wiadomo też, czy cyberataki za pomocą Stuxneta przyniosły jakieś wymierne efekty. Wiadomo natomiast, że Iran

zaczął tworzyć wojskowe jednostki specjalizujące się w cyberwalce.

Z tekstu NYT wynika, że prezydent Obama był świadomy, iż przedłużanie cyberataków wpycha Stany Zjednoczone do grupy cyberagresorów. Teraz nie będzie można powiedzieć, że ten kraj nie ucieka się do takich metod. Obama miał jednak zakładać, że środki te są uświęcane przez cel, jakim jest powstrzymanie konwencjonalnego ataku ze strony Iranu.

Współpraca z Izraelem wynikała m.in. z tego, że izraelskie służby dysponowały odpowiednią wiedzą techniczną, miały też większą wiedzę na temat tego, co się działo w Iranie. Rozpoczęto prace nad szkodnikiem i testy. Największym problemem było jednak dostarczenie robaka do ośrodka nuklearnego w Natanz. Udało się tego dokonać dzięki napędom flash.

Barack Obama, obejmując urząd prezydenta, musiał się od razu wdrożyć w zagadnienia cyberwojny. To właśnie on musiał zmierzyć się z wyzwaniem, jakim była „ucieczka" Stuxneta na wolność. To nie miało nastąpić. Błąd w kodzie sprawił, że robak skopiował się na komputer jednego z inżynierów, który potem został podłączony do internetu.

Wiadomo, że powstało co najmniej kilka rodzajów Stuxneta. Teraz temat nie wydaje się nowy, ale niedawno firma Kaspersky Lab doniosła o nowej cyberbronii, jaką jest narzędzie szpiegowskie Flame, mające cechy wspólne ze Stuxnetem.

To wszystko tworzy niewesołą sytuację. Nie będzie można już mówić np. o „złych chińskich hakerach" atakujących amerykańskie firmy. Po prostu Stany Zjednoczone podniosły cyberataki do rangi działania wojskowego.

Ciekawe jest to, że same Stany zastrzegają sobie możliwość zbrojnej odpowiedzi na tego typu atak. Można też być pewnym, że ktoś prędzej czy później tego spróbuje. Mocarstwo w dużej mierze polega na swojej infrastrukturze IT, a chętnych do

ataku jest wielu.

Opracowanie: Marcin Maj
Na podstawie: New York Times
Źródło: Dziennik Internautów