Cyberatak USA i Izraela na program atomowy Iranu

17 stycznia 2011

Kompleks Dimona położony na pustyni Negev jest znany jako pilnie strzeżone serce izraelskich badań nuklearnych. W ostatnich dwóch latach baza ta otrzymała jeszcze jedno, równie tajne, zadanie: jako poligon doświadczalny dla połączonych amerykańsko-izraelskich wysiłków do udaremnienia irańskich prób atomowych.

Za drutem kolczastym otaczającym Dimonę Izrael zbudował wirówki praktycznie identyczne jak te, które Iran umieścił w Natanz w celu wzbogacenia uranu. To właśnie w tym kompleksie testowano komputerowego wirusa Stuxnet, program, który jak się ocenia zniszczył jedną piątą irańskiego sprzętu i opóźnił zbudowanie przez Iran swoich pierwszych głowic atomowych. Amerykański ekspert w sprawie wywiadu nuklearnego podkreśla, że udało się dokonać zniszczeń właśnie dzięki testowaniu oprogramowania na praktycznie identycznym sprzęcie.

Meir Dagan, szef Mossadu, który jest oskarżany przez Irańczyków o śmierć kilku ze swoich naukowców, oświadczył niedawno, niemal równocześnie z Hillary Clinton, że irański program atomowy napotkał trudności techniczne, które opóźnią zbudowanie bomby o kilka lat.

Podczas wywiadów udzielonych przez ostatnie trzy miesiące, eksperci ze Stanów Zjednoczonych i Europy, którzy badali wirusa, opisywali go jako twór o niezwykłej budowie i o wiele większym skomplikowaniu niż ktokolwiek mógł się spodziewać, kiedy złośliwy kod zaczął krążyć po sieci w 2009.

Wiele jest jeszcze niewiadomych dotyczących wirusa, dla przykładu kto jest twórcą kodu, który wydaje się mieć wielu autorów ze wszystkich kontynentów. Po dokładnej analizie kodu znalazły się w nim elementy, które mogą naprowadzić na prawdę.

Na początku 2008 roku niemiecka firma Siemens współpracowała z amerykańskimi laboratoriami w Idaho w celu zidentyfikowania słabości w kontrolerach służących do operowania maszynami przemysłowymi, a które są wykorzystywane właśnie przez Irańczyków w ośrodkach wzbogacania uranu.

Siemens twierdzi, że były to standardowe badania mające na celu podniesienie bezpieczeństwa sprzedawanego przez nich sprzętu, jednak mimo wszystko, dzięki nim Rządowe Laboratorium w Idaho zyskało dostęp do specyfikacji sprzętu używanego przez Irańczyków. Poznali także najpopularniejsze błędy bezpieczeństwa w tym sprzęcie i wszystko wskazuje na to, że wykorzystali je już w następnym roku za pośrednictwem Stuxneta.

Wirus składa się z dwóch głównych części. Pierwszą została zaprojektowana, aby wprawić irańskie wirówki nuklearne w ruch, który by je zniszczył. Druga zapisywała jakie zwykle sygnały są wysyłane do operatorów wirówek, a następnie wysyłała dokładnie takie zapisy, tak aby na monitorach wszystko wyglądało tak jak powinno, podczas gdy naprawdę wirówki same się niszczyły.

Atak nie był jednak w pełni skuteczny. Według raportu międzynarodowych inspektorów nuklearnych większa część wirówek przetrwała. Jednak część ekspertów badających kod Stuxneta twierdzi, że zawiera on furtki, dzięki którym przyszłe wersje wirusa mogą ponowić natarcie.

Ralph Langner, niezależny ekspert komputerowy, który jako jeden z pierwszych zdekompilował kod Stuxneta twierdzi, że każdy kto dobrze go przeanalizuje może zbudować coś podobnego. Langner wyraża też obawę, że atak był tylko pierwszym rozdziałem rodzących się właśnie cyberwojen.

Oficjalnie, ani Amerykanie, ani Izraelczycy nie chcą wypowiedzieć nawet nazwy złośliwego programu, nie wspominając już o przyznaniu się do uczestniczenia w jego tworzeniu.

Jednak Izraelscy oficjele pytani o efekty pracy wirusa uśmiechają się szeroko, a Gary Samore, główny strateg Obamy, kiedy zadano mu ostatnio takie pytanie odpowiedział z uśmiechem: „Cieszę się słysząc, że mają problemy ze swoimi wirówkami, a USA wspólnie ze swoimi sojusznikami robi wszystko by jeszcze bardziej im utrudnić pracę”.

Dla wielu informatyków, ekspertów od wzbogacania uranu i byłych urzędników jest jasne, że Stuxnet jest projektem amerykańsko-izraelskim, który otrzymał pewną pomoc, świadomą czy nie, od Brytyjczyków i Niemców.

Polityczny początek programu sięga jeszcze administracji Busha. W styczniu 2009 The New York Times doniósł, że Bush zatwierdził tajny program mający na celu zniszczenie elektrycznych i komputerowych systemów w Natanz, głównym ośrodku wzbogacania uranu w Iranie. Prezydent Obama przyspieszył projekt i podobnie uczynili Izraelczycy, od dawna już szukający możliwości by przeszkodzić Iranowi w jego programie nuklearnym bez wszczynania wojny.

Wikileaks ujawniła, że dyplomacja USA zwracała szczególną uwagę, na zakupowane przez Iran kontrolery i wirus pojawił się miesiąc po depeszy opisującej dostawę układów Siemensa do tego kraju. Stuxnet został wychwycony przez Symantec, który zdziwiony odkrył, że złośliwy program nie czyni praktycznie żadnych szkód. Tajemnica zaintrygowała Langnera, który prowadził własną, małą firmę komputerową na przedmieściach Hamburga. To właśnie on odkrył, że wirus uaktywnia się jedynie jeżeli wykryje szczególną konfigurację kontrolerów spotykaną tylko w zakładach wzbogacania uranu. Okazało się, że twórcy wirusa przywiązali szczególną wagę do tego, by wirus atakował tylko konkretnie zaprogramowany w nim cel. Dla przykładu jedna z linii kodu odnosi się wyłącznie do 984 maszyn połączonych ze sobą. Co ciekawe, kiedy międzynarodowi inspektorzy odwiedzili Natanz w końcówce 2009 roku okazało się, że Irańczycy wyłączyli 984 maszyny pracujące tam jeszcze poprzedniego lata. Jednak wirus okazał się jeszcze bardziej złożony niż Langner

się spodziewał. Pewne linie kodu sprawiały, że wirus pozostawał w uśpieniu, a następnie przyspieszał obrót wirówek tak, by te zniszczyły się same, kiedy inna część programu wysyłała nagrane wcześniej sygnały o poprawnej pracy, co uniemożliwiało załączenie się systemu bezpieczeństwa i wyłączenie laboratoriów. Okazało się, że Stuxnet nie działa jak zwykłe komputerowe wirusy, ale jest zaprojektowany, by uderzyć w konkretny cel z wojskową precyzją. Do stworzenia programu potrzebna była dokładna wiedza o układach Siemensa, jak i zrozumienie w jaki dokładnie sposób działają Irańskie ośrodki wzbogacania uranu. Dokładną wiedzę na te tematy mają właśnie Izraelczycy i Amerykanie.

W listopadzie prezydent Iranu Mahmud Ahmadineżad przerwał ciszę na temat wpływu Stuxneta na program wzbogacania uranu i oświadczył, że cyberatak spowodował niewielkie problemy z niektórymi wirówkami. Najdokładniejszy raport na temat działania Stuxneta wydał prywatny Instytut Nauki i Międzynarodowego Bezpieczeństwa z Waszyngtonu. W raporcie opisane są wypadki, które zaczęły się w połowie 2009 zakończyły się na końcu tego roku w kulminacyjnym ataku, który zmusił techników do wyłączenia 984 maszyn. Raport nazwał wypadki poważnym problemem i za ich wystąpienie obwinił Stuxnet.

Opracowanie: lltr
Na podstawie: The New York Times
Nadesłano do „Wolnych Mediów”