NSA zainfekowała 50 tys. sieci na świecie

26 listopada 2013

Amerykański wywiad nie waha się używać metod kojarzonych z cyberprzestępcami. Kolejny wyciek mówi, że NSA zainfekowała 50 tys. sieci, dzięki czemu może tanio zbierać wrażliwe informacje z całego świata.

Holenderski serwis NRC ujawnił kolejne informacje pochodzące z dokumentów od Edwarda Snowdena. Wydają się one tym ciekawsze, że uzupełniają wydarzenia i wycieki, o których dużo pisano wcześniej.

Zdaniem NRC dokumenty dowodzą, że NSA zainfekowała ponad 50 tys. sieci komputerowych na całym świecie, za pomocą złośliwego oprogramowania służącego do zbierania wrażliwych informacji. Ta metoda ataku określana jest jako Computer Network Exploitation (CNE).

Według NRC na zainfekowanych komputerach umieszczane jest złośliwe oprogramowanie (określane jako „implant”), które może być w każdej chwili włączone lub wyłączone. Może ono pozostawać na komputerze w trybie „uśpienia”, co utrudnia wykrycie. Ponadto można się obawiać, że szkodniki instalowane w takich krajach, jak Brazylia czy Wenezuela, mogą być niewykrywane przez lata pomimo swojej aktywności.

NRC opublikował też mapę, która znajdowała się w dokumentach NSA. Wynika z niej, że do polskich sieci też udało się podrzucić „implanty” NSA.

Prawdopodobnie za atakami stoi wydział o nazwie TAO (ang. Tailored Access Operations), zatrudniający setki hackerów i zajmujący się szczególnie trudnymi misjami.

NRC porównuje instalowanie „implantów” przez NSA z opisywanymi

wcześnie atakami na Belgacom. Operator ten poinformował we wrześniu o znalezieniu w swojej wewnętrznej sieci nieznanego wirusa. Sprawa trafiła do prokuratury, a ta poinformowała, że wirusa mógł stworzyć ktoś dysponujący dużymi środkami finansowymi i logistycznymi. Pojawiła się sugestia, że za atakiem mogło stać jakieś państwo i od razu wskazano NSA jako potencjalnego winnego.

Później niemiecki „Spiegel" informował, że dokumenty od Snowdena zawierały informacje o tym ataku. Miała go dokonać brytyjska agencja GCHQ, która chętnie współpracuje z NSA. Instalowanie złośliwego oprogramowania miało się odbywać poprzez zwabianie pracowników firmy na sfałszowaną stronę „LinkedIn".

Trudno powiedzieć, czy brytyjski atak na Belgacom jest elementem większych działań amerykańskich. NRC podaje go jako przykład hackowania firmy przez państwo. Trzeba też mieć na uwadze, że nie tylko Amerykanie interesują się szkodnikami do zadań szpiegowskich oraz do cyberwalki. Służby krajów UE też nad tym pracują i nawet Polska najwyraźniej pracuje nad własnym szkodnikiem. Może to być bardzo tania metoda zbierania bardzo wrażliwych informacji na dużą skalę.

Autor: Marcin Maj
Źródło: Dziennik Internautów