Inwigilacja NSA? To tylko wstęp do cyberwojny

20 stycznia 2015

Amerykańskie służby specjalne nie zamierzają ograniczać się do podsłuchiwania rozmów telefonicznych. Kolejnym krokiem będzie opracowanie i wdrożenie złośliwego oprogramowania, pozwalającego na doprowadzenie do awarii systemu bankowego, systemów dostarczania energii elektrycznej i wody, transportu i innych kluczowych dla infrastruktury przeciwnika systemów. Świadczy o tym nowa partia dokumentów przekazanych dziennikarzom przez Edwarda Snowdena.

Stany Zjednoczone budują cyfrową strategię wojenną, a internetowa inwigilacja była tylko jej „fazą 0" – donosi niemiecki „Spiegel", który ujawnił kolejne dokumenty z archiwum Snowdena. Oczywiście USA są też celem ataków i dokumenty mówią, że Chińczykom udało się wykraść terabajty danych na temat samolotu F-35 Lightning II.

W ubiegłą sobotę niemiecki „Spiegel" opublikował kolejną porcję dokumentów otrzymanych od Edwarda Snowdena. Ten obszerny materiał opracowało dziewięciu dziennikarzy, a do materiału prasowego dorzucono dość dużo kopii dokumentów.

Mówiąc najogólniej, „Spiegel" stwierdza, że masowa inwigilacja NSA to był tylko początek działań, które są zorientowane na przygotowanie Stanów Zjednoczonych do wojen przyszłości, w których internet odegra kluczową rolę. Gazeta zauważa, że wiek XX przyniósł nam broń atomową, biologiczną i chemiczną, a uregulowanie użycia tej broni zajęło dekady. Z bronią cyfrową jest podobnie – już jest używana, ale nikt nie reguluje jej użycia.

Dla NSA masowa inwigilacja miała być „fazą 0" cyfrowych zbrojeń. W tej fazie zastosowano „implanty" do infiltrowania systemów wrogów albo uzyskano stały dostęp do tych systemów.

Prowadzi to do kolejnej fazy, której celem jest osiągnięcie dominacji w cyberprzestrzeni. Ta dominacja umożliwi niszczenie systemów i infrastruktur krytycznych, a więc związanych z energią, komunikacją i transportem. Trudno nie mieć tutaj skojarzeń ze Stuxnetem, który miał służyć do ataku na elektrownię atomową.

Dokumenty ujawnione przez „Spiegel" w dużej mierze dotyczą znanych już zjawisk, ale rzucają na nie nowe światło. Przykładowo opisywane wcześniej narzędzie Quantuminsert okazało się mniej skuteczne niż sądzono i zostało zastąpione narzędziem o nazwie Quantumdirk, które wstrzykuje złośliwe elementy do czatów dostarczanych przez takie strony jak Facebook i Yahoo.

Jak już wspomniano, używanie cyberbroni nie jest regulowane. To oznacza, że choć działania NSA mają znaczenie wojskowe, mogą uderzać także w cywilów. Oprogramowanie o nazwie Barnfire służy do uszkadzania serwerów, ale to niekoniecznie muszą być wojskowe cele. Oprogramowanie może być użyte m.in. do uszkodzenia systemów szpitala.

Wśród ujawnionych dokumentów znajdziemy też ciekawe informacje na temat wykorzystania urządzeń mobilnych przy różnych działaniach szpiegów. „Spiegel" wspomina, że takie urządzenie może być użyte do kradzieży danych z firm. Nieświadoma ofiara, której urządzenie zostało zainfekowane, po prostu wynosi dane z firmy, następnie są one zdalnie odzyskiwane. Szpiedzy nazywają takie osoby „mułami", ale to podejście pokazuje, że cywil staje się elementem cybernetycznych walk i nikt się tym nie przejmuje.

Oczywiście nie należy myśleć, że tylko Stany Zjednoczone interesują się szpiegowaniem i cyberwojną. Dokumenty Snowdena ujawniają również pewne osiągnięcia innych krajów oraz przypadki ataków na struktury USA. Tylko Departament Obrony miał zarejestrować 30 tys. incydentów, w ramach których zhakowano 1,6 tys. jego komputerów i 600 tys. kont

użytkowników. Dość wysoki był koszt usunięcia szkód – ponad 100 mln dolarów.

Jeden z dokumentów wskazuje na to, że chińskie służby mogły skopiować „terabajty danych" dotyczących samolotu F-35 Lightning II. Już wcześniej mówiono, że F-35 mógł być celem chińskich cyberszpiegów, ale dopiero teraz wyszło na jaw, jak wiele danych mogło wpaść w ręce Chińczyków.

Inna rzecz, że NSA i jej partnerzy z Sojuszu Pięciorga Oczu nauczyli się wykorzystywać wrogie cyberataki dla swoich celów. Zawsze przy okazji ataku istnieje możliwość zrozumienia, jak działa wróg, a nawet pozyskania jego narzędzi.

Agencja może np. przejąć już istniejący botnet czy wykorzystać technikę zwaną „fourth party collection", czyli ukraść interesujące ją dane ludziom, którzy wcześniej ukradli je celowi będącymi w polu zainteresowań NSA. Gdy Agencja wykryje, że służby innych krajów prowadzą operację cyberszpiegowską przeciwko celowi, który interesuje też NSA, potrafi „podpiąć" się pod tę operację i – w zależności od potrzeb – pasywnie podsłuchiwać lub zaimplementować własne oprogramowanie.

Przykładowo w roku 2009 jednostka NSA zauważyła wyciek danych z Departamentu Obrony. Przeprowadzono nieco pracy śledczej i w ten sposób udało się nie tylko namierzyć źródło ataku, ale też zebrać informacje wywiadowcze pozyskane w czasie innych chińskich ataków. Były wśród nich np. dane wykradzione z ONZ. Dochodzi więc do tego, że szpiedzy szpiegują szpiegów, którzy szpiegowali jeszcze kogoś. Oczywiście NSA nie ma oporów przed tym, aby wykorzystać informacje pozyskane w ten sposób. Każdy kraj spoza Pięciorga Oczu może być potencjalnym celem zbierania danych tą metodą.

Snowden zdradził m.in., że NSA wykorzystała południowokoreańską sieć szpiegowską – oczywiście bez wiedzy południowokoreańskiego wywiadu – do szpiegowania Korei Północnej. Eksperci z NSA byli w stanie skorzystać z tylnych

drzwi umieszczonych przez Koreę Południową i zainfekować cele własnym szkodliwym kodem. To najprawdopodobniej dzięki takim działaniom Amerykanie mogli bardzo szybko stwierdzić, że za ostatnie ataki na Sony odpowiada właśnie Korea Północna.

Dowiadujemy się też, że NSA stworzyła Remote Operations Center, którego zadaniem jest przeprowadzanie bardzo precyzyjnych, skomplikowanych ataków. Agencja ma też możliwości uszkodzenia infrastruktury informatycznej przeciwnika. Innym z interesujących zasobów NSA jest Tutelage. To system dedykowany obronie Pentagonu. Gdy NSA wykryje, że amerykańskie sieci wojskowe są atakowane, jest w stanie zidentyfikować poszczególne elementy systemu biorącego udział w ataku, zablokować atak, przekierować go na fałszywy cel, by wykonać szczegółową analizę oraz rozpocząć aktywne działania jak np. zniszczenie infrastruktury napastnika. Co interesujące, wszystkie te operacje są prowadzone w publicznym internecie, poza sieciami wojskowymi.

A wracając do przypadku szpiegowania Korei Północnej. Jeden z pracowników NSA zdradził, że Amerykanie byli zainteresowani szpiegowaniem sieci informatycznych komunistycznego państwa. Sami nie mieli do nich dostępu, ale wiedzieli, że Korea Południowa jest w stanie infiltrować swojego północnego sąsiada. Amerykanie odkryli, że agentom Korei Południowej udało się zainstalować specjalne układy scalone w komputerach niektórych północnokoreańskich oficjeli. NSA postanowiła skorzystać z okazji i szpiegowała Koreę Północną dzięki pracy nieświadomego niczego wywiadu Korei Południowej. Od tamtej pory sytuacja uległa jednak zmianie i NSA stworzyła własną infrastrukturę pozwalającą na szpiegowanie reżimu Kimów.

W ogólności dokumenty ujawnione przez „Spiegel” mówią jedno – służby rozwijające broń elektroniczną naprawdę robią, co chcą. Czują się nietykalne i wiedzą, że nie da się im niczego oficjalnie zarzucić. Nie ma dla nich kar, nie ma kontroli parlamentarnej, nie ma nawet żadnych międzynarodowych standardów, do których można się odnosić, oceniając ich

działania. To, co dziś nazywamy „cyberwojną”, jest tak naprawdę dzikim obszarem działań wojskowych, na którym eksperymentuje się dość swobodnie.

Można powiedzieć, że cyfrowe działania wojskowe są prowadzone bez zezwolenia i wiedzy ze strony społeczeństwa. Nikomu z nas by się nie podobało, gdyby armia podjęła działania zbrojne sama z siebie. W świecie cyfrowym to się wydaje normalne. Poprzednie wycieki mówiły, że działania w cyberprzestrzeni mogą prowadzić do takich zdarzeń, jak niezamierzone odcięcie kraju od sieci. Prawdopodobnie nikt nie jest w stanie przewidzieć wszystkich ubocznych efektów tych działań, ale wszyscy możemy ponieść ich konsekwencje.

Autorstwo: red. GR (1), Marcin Maj (2-11, 13, 17-18), Mariusz Błoński (12, 14-16)
Źródła: Głos Rosji, Dziennik Internautów, Kopalnia Wiedzy
Kompilacja 3 wiadomości na potrzeby „Wolnych Mediów”