aut. Szymon Palczewski 21.12.2020

BURZA W USA PO ATAKACH NA RZĄD. TRUMP WTÓRUJE PUTINOWI?

- Departament Skarbu, Departament Handlu, Departament Bezpieczeństwa Wewnętrznego, Departament Stanu, część Pentagonu, Departament Energii (w tym Narodowa Administracja Bezpieczeństwa Jądrowego) oraz Narodowy Instytut Zdrowia USA to obecnie instytucje rządowe, będące ofiarami szeroko zakrojonej cyberoperacji ze strony aktora państwowego.
- Zdaniem Amerykanów kampanię przeprowadziła ta sama rosyjska grupa (APT29 powiązana z FSB), która jest odpowiedzialna za cyberatak na giganta FireEye i kradzież narzędzi hakerskich. Szczegóły pod **linkiem**.
- Podczas wrogich działań wykorzystano backdoora w oprogramowaniu do zarządzania IT „Orion". Produkt firmy SolarWinds jest popularny wśród podmiotów rządowych w wielu państwach. Sama operacja to przejaw „klasycznego szpiegostwa".
- Amerykańscy politycy mówią wprost, że działania hakerów to „wypowiedzenie wojny" przez Rosję. Incydent nazwano „hackiem dekady".
- Więcej informacji na temat cyberataku można znaleźć **tutaj**.

To nie Rosja, lecz Chiny stoją za „hackiem dekady" - twierdzi kończący kadencję prezydent USA Donald Trump. Słowa głowy państwa podważają stanowisko najwyższych urzędników jego administracji, w tym sekretarza stanu Mike'a Pompeo, który oficjalnie przypisał atak Moskwie. Równocześnie Władimir Putin mobilizuje rosyjskie służby wywiadu i chwali je „zaawansowane oraz profesjonalne operacje". Kto stanie się „kozłem ofiarnym" ostatnich wydarzeń?

Szeroko zakrojona operacja hakerska wymierzona w instytucje federalne Stanów Zjednoczonych wywołała poruszenie wśród Amerykanów. Zdaniem USA za incydent odpowiada grupa Cozy Bear (APT29), działająca na zlecenie rosyjskiego FSB, a sama kampania to zaawansowane szpiegostwo, które okazało się wysoce skuteczną operacją.

Przypomnijmy, że zewnętrzny aktor państwowy uzyskał dostęp do zasobów kluczowych instytucji USA – Departamentu Skarbu, Departamentu Stanu, Departamentu Handlu, Departamentu Bezpieczeństwa Wewnętrznego, Departamentu Energii, części infrastruktury Pentagonu oraz Narodowego Instytut Zdrowia – a także naruszył bezpieczeństwo naczelnych koncernów, w tym Microsoftu. Hakerzy podczas operacji wykorzystali aktualizację popularnego oprogramowania „Orion" firmy SolarWinds do „wejścia" do wewnętrznych sieci konkretnych celów, co umożliwiło im dalsze działanie.

Środowisko specjalistów oraz politycy w USA, w tym wysocy urzędnicy państwowi, początkowo ostrożnie podchodzili do kwestii atrybucji działań hakerskich. Obecnie jednak wskazuje się, że za ataki na rządowe sieci odpowiada Kreml. W Stanach Zjednoczonych jest jednak osoba, która nie zgadza się z takimi twierdzeniami, a poprzez swoją publiczną retorykę próbuje wywołać chaos oraz podważyć zaufanie do prowadzonego dochodzenia i tym samym „ugrać" coś dla siebie.

Czytaj też: „Hack dekady". Amerykanie mówią o „wypowiedzeniu wojny" przez Rosję

„To Rosja"

Podczas piątkowego (tj. 18 grudnia br.) programu telewizyjnego „The Mark Levin Show" sekretarz stanu Stanów Zjednoczonych Mike Pompeo jako pierwszy wysoki urzędnik w państwie publicznie przypisał wrogą operację Moskwie. Na wizji podkreślił, że USA posiadają wielu wrogów, którzy chcą podważyć amerykański styl życia, struktury państwowe oraz podstawowe zasady demokracji i jednym z nich bez wątpienia jest Rosja.

> *Władimir Putin pozostaje realnym zagrożeniem dla tych z nas, którzy kochają wolność i musimy się upewnić, że jesteśmy przygotowani na to zagrożenie*
>
> *Mike Pompeo, sekretarz stanu Stanów Zjednoczonych*

Mike Pompeo podczas swojego przemówienia potwierdził, że Stany Zjednoczone doświadczyły masowego ataku na infrastrukturę informatyczną kluczowych instytucji, jednak obecnie nie może powiedzieć nic więcej, ponieważ incydent jest wciąż badany. Zdaniem przedstawiciela Waszyngtonu wiele informacji w ogóle nie zostanie ujawnionych ze względów bezpieczeństwa operacyjnego, lecz należy przekazać opinii publicznej, że atak został przeprowadzony przez Rosję.

> *To był bardzo znaczący wysiłek i (...) teraz możemy dość wyraźnie powiedzieć, że to Rosjanie zaangażowali się w tę działalność*
>
> *Mike Pompeo, sekretarz stanu Stanów Zjednoczonych*

Sekretarz stanu Stanów Zjednoczonych publicznie wyjaśnił, że w takich sytuacjach jak poważne naruszenie bezpieczeństwa państwa urzędnicy państwowi czy przedstawiciele służb naprawdę „bardzo chcieliby powiedzieć" otwarcie co się stało, aby społeczeństwo było świadome zagrożenia i bieżących wydarzeń. Jednak – jak zaznaczył Mike Pompeo – o wiele „mądrzejszym działaniem w celu ochrony Amerykanów jest spokojne zajęcie się swoimi zadaniami i obrona wolności".

> HERE'S A REVEAL: White House officials had drafted a statement to be released Friday accusing Russia of carrying out the cyber hacks, but they were blocked from doing so, a sr administration official tells @jdawsey1. Here's our story. https://t.co/BQHzaBqym9
>
> — Ellen Nakashima (@nakashimae) December 19, 2020

W tym miejscu warto podkreślić, że urzędnicy Białego Domu przygotowali specjalne oświadczenie,

którego treść odnosiła się do ataku na rządową infrastrukturę USA. Jednoznacznie oskarżono w nim Rosję o przeprowadzenie wrogiej kampanii i zaawansowane działania szpiegowskie. Dokument miał zostać opublikowany w piątek, lecz go „zablokowano" i obecnie nie wiadomo, kiedy i czy w ogóle ujrzy światło dzienne. A z pewnością uzyskałby on rozgłos nie tylko w Stanach Zjednoczonych, ale również na świecie.

Czytaj też: Największa operacja w roku? Rosyjski szturm na sieci Departamentu Skarbu oraz Handlu USA

Zasiać ziarno niepewności

Kto jest osobą, która ma odmienna zdanie na temat ataku na rząd USA? Odpowiedź brzmi: Donald Trump. Kończący kadencję prezydent USA umniejsza znaczenie incydentu, o czym świadczy jego wpis w mediach społecznościowych. Na swoim Twitterze wskazał 19 grudnia br., że wroga operacja jest kreowana na wielką kampanię przez „Fake News Media", lecz w rzeczywistości jest znacznie mniejsza.

Donald Trump zapewnił, że został „w pełni poinformowany" o incydencie i „wszystko jest pod kontrolą". Podważył równocześnie dotychczasowe doniesienia wskazujące, że to Rosja odpowiada za wrogą kampanię. Zdaniem prezydenta oskarżanie Moskwy jest przysłowiowym „najprostszym wyjściem z sytuacji", gdy cokolwiek złego dotyka Stany Zjednoczone. Jego zdaniem za operacją wymierzoną w rządową infrastrukturę „mogą stać Chiny (może!)".

To jednak nie koniec odważnych twierdzeń ze strony Donalda Trumpa. Próbował on również „ugrać coś dla siebie", wykorzystując powszechne obawy o bezpieczeństwo amerykańskiej infrastruktury i fakt, że wrogi aktor („może!" Chiny) był obecny w rządowych sieciach od co najmniej marca br., a więc… mógł przeprowadzić operację wymierzoną w systemy służące do obsługi i liczenia głosów podczas listopadowych wyborów. Kończący kadencję prezydent USA w swoim stylu obrócił najpoważniejszy atak na Stany Zjednoczone od dekady w stronę podważenia wygranej głównego kontrkandydata Joe Bidena. Zdaniem Donalda Trumpa sprawa jest jasna: hakerzy mieli dostęp również do infrastruktury wyborczej, w związku z czym z pewnością wpłynęli na wyniki, a więc należy je unieważnić.

> Former chairman of the National Intelligence Council: Trump "behaves so much like a paid Russian agent. If you look at the string of his actions & pronouncement, the only consistent interpretation that you can logically draw is that he's in their thrall."https://t.co/bNwGXp2JCY
>
> — Julia Davis (@JuliaDavisNews) December 20, 2020

W związku z tym nie może dziwić fakt, że słowa Donalda Trumpa wywołały falę komentarzy i poruszenie wśród amerykańskiej opinii publicznej. Po pierwsze, podważył on stanowisko jednego z najwyższych urzędników swojej administracji Mike'a Pompeo, który jako sekretarz stanu Stanów Zjednoczonych publicznie nazwał Rosję sprawcą ataku na rząd USA. Po drugie, podważył zebrane do tej pory dowody oraz opinie ekspertów mówiących, że to hakerzy FSB naruszyli kluczowe federalne instytucje oraz wielkich graczy biznesu. Po trzecie, wskazanie przez Donalda Trumpa na Chiny jako domniemanego sprawcę wrogiej operacji nie może dziwić. Wynika to z faktu, że dla kończącego kadencję prezydenta USA Pekin jest uznawany za „wroga numer jeden", który uparcie i agresywnie

dąży do osłabienia pozycji Stanów Zjednoczonych na arenie międzynarodowej. Aby znaleźć potwierdzenie takiego stanu rzeczy wystarczy spojrzeć na katalog nałożonych restrykcji pod adresem Państwa Środka w ostatnich latach (m.in. regularnie rozszerzana „czarna lista" czy stanowcza polityka wobec chińskich naukowców przebywających w USA). Według Donalda Trumpa amerykańska opinia publiczna kieruje się zasadą, że „wszystko co złe, to Rosja". Szkoda tylko, że sam postępuje w ten sam sposób – „wszystko co złe, to Chiny".

Co ciekawe, bardzo zbliżoną postawę do Donalda Trumpa przyjął sam rzecznik Kremla Dmitrij Pieskow. Użył on podobnych słów, co obecny jeszcze prezydent USA, wskazując, że oskarżenia pod adresem Rosji w związku z ostatnimi atakami na amerykański rząd są przejawem „ślepej rusofobii", która przejawia się przy jakichkolwiek incydentach (ponownie myśl przewodnia: „wszystko co złe, to Rosja").

Nie może dziwić fakt, że oficjalna retoryka Moskwy pozostaje niezmienna. Dmitrij Pieskow dzisiaj (tj. 21 grudnia br.) ponownie potwierdził, że Kreml nie ma nic wspólnego z naruszeniem systemów instytucji federalnych USA, a dyskusja w Stanach Zjednoczonych na temat ataków hakerskich „w żaden sposób nas nie dotyczy".

> *Rosja nie ma związku z tego typu atakami i w szczególności z ostatnimi wydarzeniami. Mówimy o tym oficjalnie i kategorycznie*
>
> *Dmitrij Pieskow, rzecznik Kremla*

Opinia publiczna w Stanach Zjednoczonych jednoznacznie ocenia, że Rosja potrzebuje Donalda Trumpa a Donald Trump Rosji. Wskazuje się, że relacje z Władimirem Putinem kończący kadencję prezydent USA traktował szczególnie, m.in. powstrzymywał się od publicznego „wskazywania palcem" na Moskwę jako sprawcę incydentów lub innych operacji.

Weteran wywiadu marynarki wojennej USA Naveed Jamali podkreślił, że „najsilniejszą cyberobroną przed Rosją" jest zmuszenie jej do poniesienia konsekwencji swoich działań. Moskwa powinna być świadoma ryzyka, co z kolei powstrzymywałoby ją od agresywnych działań. Jego zdaniem podczas prezydentury Donalda Trumpa „to się nigdy nie wydarzyło, w wyniku czego rosyjskie kampanie nasiliły się i stały się coraz bardziej bezczelne – zbliżając nas do bezpośredniego konfliktu".

Czytaj też: Pentagon na liście ofiar rosyjskiej operacji. „To klasyczne szpiegostwo"

Putin mobilizuje służby

Przemawiając na uroczystości upamiętniającej 100 lat od założenia służb wywiadu zagranicznego Rosji, prezydent tego kraju Władimir Putin podkreślił, że agenci są wyjątkowo ważni dla ochrony całego państwa, a ich praca jest gwarancją „suwerenności, demokracji i niezależnego rozwoju Rosji". Słowa, które padły podczas uroczystości mają szczególny wydźwięk w obecnej sytuacji, kiedy Moskwa jest oskarżona o atak na rząd Stanów Zjednoczonych i zaawansowaną kampanię „klasycznego szpiegostwa".

> *Życzę powodzenia tym, którzy bronią Rosji przed zagrożeniami zewnętrznymi i wewnętrznymi, opowiadają się za naszą suwerennością i interesami narodowymi oraz dla których bezpieczeństwo i dobrobyt Ojczyzny były i zawsze będą zobowiązaniem na całe życie*
>
> *Władimir Putin, Prezydent Rosji*

Oczywiście w ramach swojego wystąpienia Prezydent Rosji Władimir Putin rozpoczął od złożenia „serdecznych gratulacji" dla wszystkich osób, które pracowały lub nadal pracują „w tej kluczowej dla państwa dziedzinie". Następnie jednoznacznie ocenił, że oficerowie wywiadu wnoszą nieoceniony wkład w zapewnienie bezpieczeństwa kraju i niejednokrotnie bezinteresownie wykonują najtrudniejsze zadania, których efekty wpływały „nawet na bieg naszej historii i świata".

Władimir Putin stanowczo zaapelował do przedstawicieli rosyjskiego wywiadu o konieczność dalszego reagowania na zmieniającą się sytuację międzynarodową. Prezydent oczekuje od agentów szczególnego zaangażowania w identyfikowanie i neutralizowanie potencjalnych zagrożeń dla państwa.

> *Bez wątpienia, gdy agencje bezpieczeństwa sprawnie wykonują swoje zadania, podporządkowane prawu i naszym interesom narodowym, ich praca miała i zawsze będzie miała dla Rosji nadrzędne znaczenie*
>
> *Władimir Putin, Prezydent Rosji*

Bardzo ciekawe wydają się słowa Władimira Putina – tu cytat: „Musimy dalej rozwijać sukcesy osiągane przez agencje kontrwywiadu. Wiem z pierwszej ręki, o czym tutaj mówimy, i pochwalam te zaawansowane oraz profesjonalne operacje". Fragment ten stanowi przesłanie skierowane do państw uznawanych przez Moskwę za przeciwników. Ich wydźwięk mówi wprost: „Rosyjskie służby są wśród Was a ich działania są skuteczne, więc uważajcie". Nie bez przyczyny słowa Władmira Putina krążą w Stanach Zjednoczonych i stanowią przedmiot analizy, zwłaszcza w kontekście ostatnich wydarzeń.

Czytaj też: „Słodka zemsta" rosyjskiego FSB na Amerykanach? Zhakowano giganta cyberbezpieczeństwa

„Polecą głowy"?

Kampania hakerska, w której skutecznie naruszono infrastrukturę rządową USA wywołała szok wśród najważniejszych osób w państwie, polityków, ekspertów i samych obywateli. Pojawiły się również pytania i wątpliwości dotyczące kondycji cyberbezpieczeństwa państwa. Niemalże od początku nagłośnienia incydentu obecne są głosy, że jakość rozwiązań z zakresu ochrony infrastruktury oraz wykrywania wrogiej aktywności w sieciach nie jest wystarczająca. Zdaniem Amerykanów rząd regularnie wydaje miliardy dolarów na nowe cybernarzędzia, które – jak pokazały ostatnie wydarzenia

– hakerzy bez większego wysiłku są w stanie „przechytrzyć”.

Środowisko ekspercie, które zajmuje się operacją hakerską wskazuje, że działania wrogich podmiotów wpisują się w katalog szeroko zakrojonej operacji „klasycznego szpiegostwa”. Sektor prywatny, w tym amerykański gigant cyberbezpieczeństwa FireEye, mówi o pierwszym sukcesie w neutralizacji kampanii poprzez „wyłączenie” podstawowego narzędzia przeciwnika. Wszystkie wysiłki sprowadzają się do ograniczenia broni hakerów, lecz nadal nie zostali oni „usunięci” z naruszonych sieci i systemów. Jest to szczególnie niebezpieczne, ponieważ w takiej sytuacji w każdej chwili wróg obecny w infrastrukturze może przekształcić swoją operację szpiegowską w destrukcyjny atak, który zniszczy lub zakłóci działanie np. wojskowych sieci (obecność w części systemów Pentagonu) czy systemów powiązanych z amerykańską bronią nuklearną (obecność w systemach Narodowej Administracji Bezpieczeństwa Jądrowego – Departament Energii). Należy mieć na uwadze, że hakerzy rosyjskiego FSB (Cozy Bear, APT29) nie słyną z tego typu „niszczycielskich działań”, jednak przejście z operacji szpiegowskiej do bardziej destrukcyjnej kampanii jest proste i realne.

Ze względu na skalę zagrożenia coraz więcej mówi się w Stanach Zjednoczonych o konieczności zmiany podziału kierownictwa nad NSA (ang. National Security Agency) i Cyber Command. Obecnie zwierzchnikiem obu tych podmiotów jest gen. Paul Nakasone.

Wyżsi urzędnicy w Pentagonie, w tym zastępca sekretarza obrony ds. wywiadu i bezpieczeństwa Ezra Cohen-Watnick, naciskają, aby Agencja znalazła się pod cywilną kontrolą jeszcze przed zakończeniem kadencji administracji Donalda Trumpa. Plan zmiany w obszarze kierownictwa nad kluczowymi podmiotami dla bezpieczeństwa USA pojawił się w momencie nagłośnienia ataku na rząd USA. Jest on wspierany przez pełniącego obowiązki sekretarza obrony Chrisa Millera i ma stanowić „odkurzoną” wersję projektu roszad, która pojawiła się w Pentagonie już wcześniej.

Wydaje się, że silne forsowanie koncepcji podziału kierownictwa nad NSA i Cyber Command to przejaw chęci znalezienia „kozła ofiarnego” za ostatnie wydarzenia, którym miałby być gen. Paul Nakasone. Według części obecnych i byłych urzędników Departamentu Obrony USA dowódca obu podmiotów ma odpowiadać za „oczywiste uchybienia”, w tym w zakresie wykrycia działalności wroga w rządowych sieciach, co ostatecznie doprowadziło do poważnego naruszenia bezpieczeństwa Stanów Zjednoczonych. Większość specjalistów jest jednak zdania, że gen. Paul Nakasone nie ponosi żadnej winy za atak na rząd, a jest to po prostu efekt systemowych problemów związanych z cyberobroną, które obejmują całą administrację.

Jednym z przydatnych rozwiązań byłoby wprowadzenie regulacji, która nakazywałaby informowanie o naruszeniach danych w odniesieniu nie tylko do sektora prywatnego, ale również agencji rządowych. Mowa tu o propozycji uchwalenia ustawy federalnej o powiadamianiu w przypadku tego typu incydentów, jaka zobowiązywała wszystkie podmioty do ujawniania wszelkich wskaźników zagrożenia tak szybko, jak to tylko możliwe – oczywiście z poszanowaniem bezpieczeństwa prowadzonego dochodzenia.

Skąd taki pomysł? Warto zwrócić uwagę, że pierwszym podmiotem, który ujawnił operację hakerów w rządowych sieciach był amerykański koncern FireEye (sam wcześniej padł ofiarą tego samego podmiotu). Gdyby władze firmy nie podjęły tej odważnej decyzji o publicznym poinformowaniu o ataku i przedstawieniu analizy incydentu, nikt by o niej nie usłyszał. To dzięki sektorowi prywatnemu świat ujrzał zaawansowaną operację, którą już teraz została okrzyknięta „hackiem dekady”. Wprowadzenie prawa, które nakładałoby obowiązek ujawniania tego typu zdarzeń, a nie trzymanie ich w tajemnicy, pozwoliłoby uniknąć chaosu medialnego i skondensowało przekaz kierowany do opinii publicznej.

Czytaj też: Brytyjczycy kolejnym celem operacji Rosjan? Trwa audyt rządowych sieci