SENAT
RZECZYPOSPOLITEJ
POLSKIEJ

X kadencja

Zapis stenograficzny

z posiedzenia Komisji Nadzwyczajnej do spraw wyjaśnienia przypadków nielegalnej inwigilacji, ich wpływu na proces wyborczy w Rzeczypospolitej Polskiej oraz reformy służb specjalnych (2.)

17 stycznia 2022 r.

Warszawa 2022 r.

Porządek obrad:

1. Wysłuchanie ekspertów Johna Scotta-Railtona oraz Billa Marczaka z The Citizen Lab na Uniwersytecie w Toronto.

(Początek posiedzenia o godzinie 14 minut 02)

(Posiedzeniu przewodniczy przewodniczący Marcin Bosacki)

PRZEWODNICZĄCY
MARCIN BOSACKI

Dzień dobry państwu.

Otwieram posiedzenie komisji, drugie posiedzenie komisji nadzwyczajnej. Pierwsze, prowadzone przez marszałka Tomasza Grodzkiego, miało za zadanie wyłącznie wybranie przewodniczącego komisji i odbyło się w ubiegły czwartek.

Informuję, że posiedzenie komisji jest transmitowane w internecie.

Chciałbym sprawdzić, czy wszyscy senatorowie, którzy chcieli wziąć udział w posiedzeniu komisji w sposób zdalny, zostali już włączeni do posiedzenia.

(*Wypowiedź poza mikrofonem*)

Dziękuję bardzo.

Czy goście, którzy chcieli uczestniczyć w posiedzeniu komisji w sposób zdalny, zostali już włączeni do posiedzenia również?

(*Wypowiedź poza mikrofonem*)

Też dziękuję bardzo.

Szanowni Państwo, Senat, powołując komisję nadzwyczajną do spraw nielegalnej inwigilacji, zlecił nam 3 zadania.

Pierwszym z tych zadań jest ustalenie, co się stało: czy, w jaki sposób, na jaką skalę, wobec kogo stosowano w Polsce system Pegasus – który w zgodnej opinii ekspertów jest bronią cybernetyczną.

Po drugie, ustalenie wpływu tych działań, tych nielegalnych przypadków inwigilacji na wybory, zwłaszcza wybory w 2019 r. – oczywiście jeśli będą nowe dane, to również na wybory wcześniejsze lub późniejsze.

Wreszcie, po trzecie, na wypracowanie propozycji prawnych, w tym ustawowych, na reformę służb specjalnych, tak by kontrola nad nimi była wyraźniejsza i by tego typu przypadki nielegalnej inwigilacji nie mogły się powtarzać w przyszłości albo przynajmniej były dużo mniej prawdopodobne.

Chciałbym w tej chwili powiedzieć, że komisja w toku naszych przygotowawczych działań koordynacyjnych zadecydowała, że najpierw zajmiemy się tym pierwszym zagadnieniem, czyli co się stało, czy, w jaki sposób, wobec kogo, jak często stosowano system Pegasus. Dlatego też pierwszymi z wysłuchiwanych, zaproszonych i wysłuchiwanych przez komisję osób będą eksperci, którzy stwierdzili używanie systemu Pegasus w Polsce wobec senatora Krzysztofa Brejzy, szefa kampanii wyborczej głównej siły opozycji w 2019 r., wobec mecenasa Romana Giertycha i wobec prokurator Ewy Wrzosek. Za parę minut będziemy rozmawiać z ekspertami Instytutu Badawczego Citizen Lab z Toronto w Kanadzie.

Później będziemy zapraszać zarówno ekspertów od spraw cybernetycznych, jak i byłych funkcjonariuszy służb specjalnych, prawników, oczywiście samych poszkodowanych tą aferą, ale też wysokich urzędników państwowych, którzy kierowali, kierują, nadzorowali bądź nadzorują służby specjalne.

Chciałbym jednocześnie powiedzieć, że dzisiejsze posiedzenie miało mieć 2 punkty. Poza wysłuchaniem ekspertów z instytutu badawczego Citizen Lab z Toronto mieliśmy również wysłuchać prof. Jerzego Kosińskiego, który jest wybitnym specjalistą od spraw cyberbezpieczeństwa. Był wykładowcą szkoły policyjnej w Szczytnie, a w tej chwili jest profesorem nadzwyczajnym Zakładu Systemów Bezpieczeństwa Akademii Marynarki Wojennej w Gdyni.

Do 2018 r. pełnił służbę w Policji, zajmując się cyberprzestępczością, dowodami cyfrowymi, białym wywiadem internetowym. Odchodził na emeryturę jako prorektor do spraw studiów Wyższej Szkoły Policji w Szczytnie. Prowadził m.in. szkolenia z zakresu cyberprzestępczości dla służb innych krajów, w tym Armenia czy Mołdawia, a od 2 lat, jak już mówiłem, kieruje Morskim Centrum Cyberbezpieczeństwa działającym przy Akademii Marynarki Wojennej. Chcieliśmy zadać panu profesorowi pytania o to, jak działa Pegasus, w jaki sposób on został do Polski sprowadzony, także chcieliśmy zapytać o sposób tego sprowadzenia. Pan profesor się zgodził na spotkanie z komisją, potwierdził to. 2 godziny temu poinformował mnie, że niestety rezygnuje ze stawienia się przed komisją z powodu, jak to określił, rozmów z przełożonymi, którzy mu to stanowczo odradzali. Ja chciałbym wyrazić najdalej idące ubolewanie z tego powodu i zapytać członków komisji, czy mają jakiś komentarz do tego.

SENATOR
SŁAWOMIR RYBICKI

Dziękuję, Panie Przewodniczący.

Proszę państwa, komisja senacka działa na podstawie prawa w interesie publicznym. I zgodnie z polskimi przepisami prawa, w tym Regulaminu Senatu, na żądanie komisji albo przewodniczącego komisji w sprawach będących przedmiotem jej zakresu działania przedstawiciele Rady Ministrów i wszystkich instytucji państwowych, samorządowych oraz powiązanych czy to kapitałowo, czy też formalnie, prawnie z budżetem państwa... Te osoby są obowiązane do współpracy z komisją, a w szczególności przedstawiania informacji, wyjaśnień, opinii w formie pisemnej lub przy wykorzystywaniu innych nośników, przekazywania materiałów i czynnego udziału w posiedzeniach komisji. Radę Ministrów może reprezentować na posiedzeniu przedstawiciel.

Proszę państwa, uważamy, że ten przypadek, ten incydent jest przejawem strachu władzy publicznej w Polsce przed wyjaśnieniami, które mają fundamentalne znaczenie dla oceny stanu praworządności w Polsce. I mamy nadzieję, że nieformalny wpływ na przyszłych naszych świadków nigdy nie będzie więcej miał miejsca. Dziękuję bardzo.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

W związku z tym porządek naszego dzisiejszego posiedzenia obejmuje 1 punkt, czyli wysłuchanie specjalistów, badaczy z ośrodka Citizen Lab w Uniwersytecie w Toronto.

Czy jest zgoda komisji na taki porządek obrad?

(*Wypowiedzi w tle nagrania*)

Dziękuję bardzo.

Przedstawię więc naszych pierwszych gości.

Czy mamy z nimi połączenie? Mam nadzieję, że mamy.

Pan John Scott-Railton jest starszym pracownikiem naukowym w laboratorium badawczym Citizen Lab w Munk School na Uniwersytecie w Toronto, gdzie prowadzi dochodzenia w sprawie zagrożeń dla społeczeństwa obywatelskiego. Od 10 lat analizuje i wydaje publikacje na temat złośliwego oprogramowania i kampanii dezinformacyjnych. Pan Scott-Railton prowadził dochodzenia w sprawie operacji przypisywanych m.in. Rosji, Iranowi, Syrii i ISIS, a także współpracował przy śledztwach dotyczących nadużywania oprogramowania szpiegowskiego na całym świecie. John był m.in. współpracownikiem Google Ideas i Jigsaw. Ukończył część studiów doktoranckich na Uniwersytecie Kalifornijskim w Los Angeles, a uprzednio studiował na Uniwersytecie Chicagowskim, na Uniwersytecie Michigan. Jego prace są regularnie publikowane w wielu mediach w Kanadzie, w Stanach Zjednoczonych i w innych krajach.

Drugim naszym ekspertem będzie Bill Marczak, pracownik naukowy w laboratorium badawczym Citizen Lab na Uniwersytecie w Toronto. Pracował poprzednio jako naukowiec po studiach doktoranckich na Uniwersytecie Kalifornijskim w Berkeley, gdzie uzyskał tytuł doktora informatyki. Praca pana Marczaka skupia się na nowych technologicznych zagrożeniach dla wolności internetu, w tym na nowych narzędziach cenzury i inwigilacji. Prace doktora Marczaka były omawiane m.in. w „Vanity Fair", „New York Times", „Washington Post" i CNN.

Chciałbym zapytać panów na wstępie, jak to się stało, że Citizen Lab, renomowana jednostka badawcza jednego z najlepszych na świecie uniwersytetów, zajęła się programem Pegasus i, po

drugie, programem Pegasus i jego obecnością w Polsce.

Bardzo proszę, który z panów odpowie?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Przede wszystkim, Panie Senatorze, bardzo dziękujemy za zaproszenie nas. Cieszymy się, że możemy się spotkać i odpowiedzieć na pytania komisji.

Nasza praca dotycząca Pegasusa zaczęła się wiele lat temu. Po raz pierwszy zaczęliśmy badać Pegasusa w 2016 r...

(*Przewodniczący Marcin Bosacki*: Przepraszam, to jest pan John Scott-Railton.)

Czy słyszą mnie państwo?

(*Przewodniczący Marcin Bosacki*: Tak, słyszymy.)

Tak więc nasza praca w sprawie Pegasusa rozpoczęła się w 2016 r., wraz z pierwszym prowadzonym przez nas śledztwem, i od tego czasu przeprowadziliśmy w Citizen Lab dziesiątki dochodzeń dotyczących nadużyć związanych z wykorzystaniem oprogramowania szpiegującego Pegasus dosłownie na całym świecie. Z polskim przypadkiem zetknęliśmy się na 2 sposoby. W 2018 r. publikowaliśmy globalny raport zawierający analizę tego, gdzie na całym świecie znajdowali się, jak podejrzewaliśmy, klienci Pegasusa, i w ramach tego dostrzegliśmy klienta, który był aktywny wyłącznie w Polsce. Zwróciło to naszą uwagę i nadaliśmy temu klientowi nazwę. Następnie w ubiegłym roku firma Apple wysłała powiadomienia do wielu osób, które padły ofiarą konkretnego exploita. Za pośrednictwem Twittera dowiedzieliśmy się, że jedna z osób, które otrzymały takie powiadomienie, Ewa Wrzosek, znajdowała się w Polsce. Ta sprawa od razu przykuła naszą uwagę. Byliśmy przyzwyczajeni do tego, że prowadziliśmy dochodzenia w przypadku państw dyktatorskich, więc zastanawiało nas to, co dzieje się w państwie demokratycznym, kiedy celem tego rodzaju oprogramowania szpiegującego jest prokurator. I od tego rozpoczęliśmy badania dotyczące użycia Pegasusa w Polsce. Głównie korzystaliśmy tu z kryminalistycznych metod śledczych, próbując ustalić, czy istnieją inne przypadki podobne do sprawy pani Ewy.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Rozumiem, że badali państwo również przypadek chyba najbardziej politycznie w Polsce bulwersujący, mianowicie szefa kampanii jednej z sił opozycyjnych, senatora Krzysztofa Brejzy. Wiemy już z jego informacji, które on podał, że wykryliście państwo 33 ataki oprogramowaniem Pegasus na jego telefon. Czy są jakieś nowe wiadomości w tej sprawie? Czy macie państwo coś nowego do dodania poza tą ogólną informacją o 33 atakach?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Tak, rzeczywiście dziś po raz pierwszy możemy publicznie potwierdzić, że mamy dowody kryminalistyczne wskazujące na to, że faktycznie zostały z urządzenia senatora wykradzione dane. Byliśmy w stanie dostrzec dowody na to, że znaczne ilości danych wychodziły z tego telefonu, w tym także w momentach wrażliwych pod względem politycznym.

PRZEWODNICZĄCY
MARCIN BOSACKI

Czy może pan powiedzieć coś bliżej na ten temat? Jakiego typu dane to są? Jaka jest ilość tych danych? Jak często pobierano te dane?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dostrzegamy liczne ślady danych wychodzących z urządzenia. Wciąż jesteśmy w trakcie

analiz, więc nie mogę w tej chwili mówić konkretnie o typach danych ani o ich ilości. Jesteśmy jednak przekonani o słuszności tego ustalenia i uważamy, że potwierdza ono fakt, iż senator był objęty rozszerzoną inwigilacją.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Bardzo proszę teraz moich kolegów, członków komisji, o zadawanie pytań.

Bardzo proszę, senator Sławomir Rybicki.

SENATOR
SŁAWOMIR RYBICKI

Dziękuję bardzo.

Chciałbym zapytać panów, kontynuując wcześniejszy wątek, o inwigilowanie senatora Brejzy. Ale przede wszystkim gdyby zechcieli państwo nam opisać istotę działania Pegasusa... Na czym polega jego szczególna funkcja, która, jak się okazuje, poza podsłuchiwaniem może też być wykorzystywana w wielu innych aspektach, do kreowania różnych wydarzeń? Jakie to ma znaczenie dla ewentualnego wykorzystywania tych narzędzi w procesie wyborczym w Polsce? Bardzo bym prosił o odpowiedź, o istotę działania tego Pegasusa, w tym kontekście właśnie.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję za to pytanie, Panie Senatorze. Oprogramowanie szpiegujące Pegasus w swej istocie jest wszechstronnym narzędziem szpiegowskim. Można myśleć o tym tak: ma się w kieszeni telefon, który przekształcił się w informatora i działa przeciwko nam. To wszystko, co użytkownik telefonu może robić – używać czatu, korzystać z szyfrowanych wiadomości, wykonywać połączenia telefoniczne, robić notatki czy rodzinne fotografie – wszystkie te czynności stają się podatne na monitorowanie przez Pegasusa. Ponadto Pegasus ma możliwość włączania w sposób zdalny, potajemnie, mikrofonu i kamery w urządzeniu, skutecznie zmieniając telefon w coś w rodzaju, powiedziałbym, pluskwy w pokoju, podsłuchu. Ale to nie wszystko. Pegasus umożliwia operatorowi również wykradanie danych uwierzytelniających lub tokenów używanych przez telefon do uzyskiwania dostępu do kont internetowych, co oznacza, że nawet po zakończeniu infekowania urządzenia Pegasusem nadal umożliwia on dostęp do tych kont internetowych. Można o nim myśleć jako o włamywaczu, który nie tylko włamał się do domu i, chowając się w szafie, podsłuchuje i obserwuje rodzinę, ale także zabiera do swojej kieszeni klucze do waszego domu, klucze do wszystkich innych waszych domów i posiadłości. Jest to więc bardzo wszechstronne narzędzie inwigilacji, wyjątkowo inwazyjne. W wielu przypadkach nasuwa się pytanie, czy jego inwazyjność jest kompatybilna z konstytucyjnymi uprawnieniami do inwigilacji w krajach demokratycznych.

SENATOR
SŁAWOMIR RYBICKI

To mam jeszcze jedno pytanie z tym związane. Czy macie państwo jakieś narzędzie, które stwierdza bez wątpliwości, że użyty środek operacyjny jest właśnie programem Pegasus, a nie innym programem?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. Tak, mamy narzędzie, którego używamy i które pozwala nam potwierdzić, że do telefonu włamano się za pomocą Pegasusa – a nie innego rodzaju oprogramowania szpiegującego lub innej technologii – bo wyszukuje ono charakterystyczne ślady kryminalistyczne. Np. osoby piszące Pegasusa, twórcy Pegasusa, dokonują pewnych wyborów, tworząc oprogramowanie szpiegujące, nadają pewne nazwy różnym komponentom, stosują pewne techniki w celu ukrycia działania oprogramowania szpiegującego lub usunięcia

śladów jego aktywności, a wszystko to pozostawia ślady, niejako sygnatury, które możemy z dużą pewnością powiązać z oprogramowaniem szpiegującym Pegasus firmy NSO Group, w odróżnieniu od jakiegokolwiek innego oprogramowania szpiegującego.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Drobne dopytanie. Czy w czasie, kiedy zaczynano stosować Pegasusa w świecie, ale też w Polsce, w 2017, 2018 r., ten system był wówczas uznawany za niewykrywalny – tak? Czy dobrze mówię?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Zgadza się, Panie Senatorze. Był promowany jako niewykrywalny. Ale, jak wykazały nasze badania, w rzeczywistości jest wykrywalny.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Senator Magdalena Kochan. Bardzo proszę.

SENATOR
MAGDALENA KOCHAN

Bardzo dziękuję, Panie Przewodniczący.

Państwo zainteresowaliście się Polską i tym, że na jej terenie działa ta cybernetyczna broń, właściwie – z tego, co zrozumiałam przed chwilą – w związku z inwigilacją pani prokurator Ewy Wrzosek. Dzisiaj wiemy, że także senator, przewodniczący, szef kampanii wyborczej jednej z partii starającej się o miejsce w parlamencie, ale także adwokat, pan Roman Giertych, byli przedmiotem tych działań. Moje pytanie brzmi tak: czy Polska różni się – a jeżeli tak, to czym się różni – w używaniu tej broni od innych państw, na terenie których czy które to państwa przez swoje służby specjalne tej cybernetycznej broni używają? Czy się różni, a jeśli tak, to czym?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Pani Senator, dziękuję za pytanie. Mogę powiedzieć, że mamy dwie obserwacje dotyczące przypadków, które do tej pory wykryliśmy w Polsce. Moje pierwsze spostrzeżenie jest takie, że działania wymierzone w wiele osób, których przypadki objęliśmy śledztwem w Polsce, zwłaszcza w mecenasa Giertycha i w senatora Brejzę, były szeroko zakrojone i miały agresywne tempo. Szczególnie w przypadku senatora Brejzy widzimy, że był on brany na cel raz za razem, wielokrotnie w 2019 r., co według nas świadczy o silnym dążeniu operatora Pegasusa do regularnego sprawdzania, co robi dana osoba. W tamtym czasie był to dla nas jeden z bardziej agresywnych przypadków, jakimi się zajmowaliśmy.

Druga sprawa, o której chciałbym powiedzieć: wiele naszych dochodzeń dotyczy nadużywania Pegasusa w krajach dyktatorskich. Kiedy więc publikowane są przez nas lub przez inne organizacje materiały potwierdzające użycie tam Pegasusa, pojawiają się zaprzeczenia, do których jesteśmy już przyzwyczajeni. Jesteśmy przyzwyczajeni do tego, że takie państwo stara się zminimalizować wyniki tych badań lub odwrócić od nich uwagę, a w innych przypadkach po prostu je ignoruje. Polska jest jednak krajem demokratycznym, z silnymi tradycjami praworządności. I zaskoczyło mnie to, że gdy obserwowaliśmy oficjalne wypowiedzi różnych przedstawicieli polskiego rządu, bardzo trudno było nam w pełni zrozumieć ich stanowisko w tej sprawie. W rzeczywistości wciąż staramy się zrozumieć niektóre elementy ich wypowiedzi co do tej kwestii.

Chciałbym również zauważyć, że z pewnym niepokojem obserwujemy niektóre doniesienia dotyczące dalszych działań w tej sprawie, zwłaszcza co do sytuacji senatora Brejzy oraz jego rodziny i ojca.

(*Senator Magdalena Kochan*: Czy mogę dopytać?)

PRZEWODNICZĄCY
MARCIN BOSACKI

Proszę bardzo, Pani Senator.

SENATOR
MAGDALENA KOCHAN

Bardzo dziękuję.

Z pana odpowiedzi zrozumiałam tyle, że na tle innych służb, niepolskich, używających Pegasusa, te ataki przy jego pomocy stosowane szczególnie na polityka, pana senatora Brejzę, były czymś wyjątkowym, nawet w skali innych państw używających tego rodzaju broni. Czy tak? I czy znane są panu, panom, przypadki, gdzie ta broń jest stosowana tak bezpośrednio wobec osób, które... Senator Brejza to oczywiście polityk i szef kampanii wyborczej – tutaj kontekst polityczny jest dość ewidentny. Ale jest w tym też adwokat, którego tajemnica adwokacka właściwie obowiązuje wszystkich i nikt nigdy nie ma prawa z tajemnicy adwokackiej kogokolwiek zwolnić, czy prokurator, która, prowadząc niejedno śledztwo, stojąc na straży naszego bezpieczeństwa, będąc w ten sposób atakowana, mogłaby nie prowadzić go we właściwy sposób czy nie móc doprowadzić do skazania osób podejrzanych, którym po śledztwie mogłaby udowodnić przestępstwo. Czy tego rodzaju przypadki w innych krajach są w ogóle przez państwa notowane? Dziękuję.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Pani Senator, dziękuję za pytanie. Sprawa polska jest wyjątkowa, po części ze względu na polski kontekst, na pewno ze względu na intensywność ataków, zwłaszcza w przypadku senatora Brejzy, ale także z racji ataków na prokuratora w systemie demokratycznym. Chyba mogę powiedzieć, że nie spotkałem się w naszych badaniach z żadnym innym przypadkiem, który byłby podobny do tego. Ogólnie rzecz biorąc, widzimy, że Pegasus jest często używany w kontekście politycznym, co jest oczywiście uderzające, gdy brać pod uwagę to, że narzędzie to jest promowane jako przeznaczone do wykrywania przestępstw i terroryzmu.

Powinienem też podkreślić, że zgodnie z naszym rozeznaniem co do programu Pegasus, gdy jest on sprzedawany klientowi, kupowana jest określona liczba licencji, np. 10 lub 20, i licencje te, jak sądzimy, określają liczbę jednoczesnych infekcji, których może dokonać operator Pegasusa. Oznacza to, że jeśli kupi się 10 licencji, to w tym samym czasie można aktywnie monitorować poprzez Pegasusa tylko te 10 osób. Jest tu oczywista implikacja: przez cały czas, gdy senator Brejza był bezpośrednio inwigilowany poprzez Pegasusa, ta jedna licencja nie mogła być wykorzystywana do deklarowanego celu Pegasusa, jakim jest walka z przestępczością i terroryzmem. Jest to dla mnie uderzające, zwłaszcza że wiemy, iż Pegasus został zakupiony za publiczne pieniądze. Dziękuję za pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Kto z państwa senatorów?
Senator Jacek Bury. Bardzo proszę.

SENATOR
JACEK BURY

Ja chciałbym zapytać: czy są państwo w stanie powiedzieć nam, ile krajów demokratycznych korzysta z Pegasusa? Czy macie takie dane? Czy takie kraje przyznały się do tego? Jeżeli tak, to czy w tych krajach są procedury nadzoru nad używaniem tego typu broni cybernetycznej? To właściwie takie podstawowe moje pytanie, za chwilę dopytam jeszcze o inne rzeczy.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za to zasadnicze pytanie. Wiemy o innych przypadkach, o tym, że Pegasus jest podobno wykorzystywany przez służby bezpieczeństwa w innych krajach

demokratycznych, aczkolwiek znaleźliśmy w niektórych publicznych doniesieniach dotyczących tych przypadków pewne powody do niepokoju. To, co chciałbym tu zaznaczyć, to fakt, że rynek tego rodzaju oprogramowania szpiegującego i jego wykorzystanie są na ogół otaczane tajemnicą. Nie sądzę, by ktokolwiek kwestionował to, że policja powinna być władna pod względem technologicznym do ścigania poważnych przestępstw, ale niepokój wiąże się z tym, że Pegasus jest tak wyrafinowaną technologią, że łatwo może zostać wykorzystany w niewłaściwy sposób. I sądzę, że stale przekonujemy się – w tym przypadku, niestety, w kraju demokratycznym – że pokusa nadużywania go jest bardzo duża. Dlatego też absolutnie konieczny jest ścisły nadzór.

SENATOR
JACEK BURY

Czyli rozumiem, że w tych krajach demokratycznych, które używają zgodnie z licencją, z potrzebą, przez służby typu wywiad, kontrwywiad... Te kraje mają opracowane procedury i te procedury, według waszej wiedzy, są raczej przestrzegane?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

To jest bardzo dobre pytanie, Panie Senatorze. Często nie jesteśmy w stanie stwierdzić, czy procedury są przestrzegane. Pytanie oczywiście brzmi: czy istnieją dowody wskazujące na to, że procedury mogą nie być przestrzegane? Sądzę, że spotykamy się dziś z państwem częściowo dlatego, że te 3 przypadki, o których rozmawiamy, to są takie czerwone flagi ostrzegawcze, które wskazują na możliwość nieprzestrzegania procedur i brak nadzoru.

SENATOR
JACEK BURY

I jeszcze takie pytanie mam odnośnie senatora Krzysztofa Brejzy, który był szefem sztabu wyborczego Platformy Obywatelskiej. Czy macie dowody na to, że jego monitorowanie, użycie wobec niego Pegasusa, wiązało się np. z uruchamianiem kamery, która w danym momencie nie była aktywna, czy mikrofonu, który w danym momencie nie był aktywny?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za to pytanie. Wciąż analizujemy szczegóły każdego przypadku i w tej chwili nie możemy podać więcej naszych spostrzeżeń do publicznej wiadomości.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję...

SENATOR
JACEK BURY

Czy są jakieś dowody...
(*Przewodniczący Marcin Bosacki*: Panie Senatorze...)
Ostatnie, krótkie pytanie. Czy są jakieś dowody, czy posiadacie dowody, że modyfikowano informacje czy pliki w telefonie pana senatora Brejzy?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za to pytanie. Kiedy po raz pierwszy zaczęliśmy badać sprawę senatora Brejzy, przeżyłem moment déjà vu. Kilka lat wcześniej współprowadziłem śledztwo w sprawie hakowania przez rosyjski rząd. Chodziło o znaną wszystkim grupę hakerską powiązaną z poważnymi atakami rządu rosyjskiego na Stany Zjednoczone i Europę. Fascynujące w tej sprawie było to, że zaobserwowaliśmy, iż

hakerzy uzyskali dostęp do kont poczty elektronicznej kilku osób, wykradli e-maile, a następnie zobaczyliśmy, że treść tych e-maili została lekko zmodyfikowana i upubliczniona. Stanowiło to przykład aktywnych działań służących dezinformacji. Z racji mojego rozeznania w sprawie senatora Brejzy w 2019 r., od razu przypomniała mi się tamta sytuacja. A z uwagi na ujawnienie wiadomości rzekomo pochodzących od senatora Brejzy, w szerokim stopniu zgłaszano je jako zmanipulowane. Ta sprawa przypomniała mi o dezinformacji i o rosyjskich aktywnych działaniach jej służących.

Powiem tak: kiedy telefon zostanie zhakowany za pomocą Pegasusa, informacje w nim zawarte z pewnością stają się podatne na manipulacje. W każdym przypadku, gdy urządzenie zostanie zainfekowane tego rodzaju oprogramowaniem szpiegującym, daje ono zdalnemu, tajnemu operatorowi dostęp do tego urządzenia, dzięki czemu może on oczywiście wprowadzać informacje na to urządzenie. Rodzi to oczywiście poważne obawy dotyczące wykorzystania wszelkich materiałów, które mogły zostać wykradzione z tego urządzenia, oraz tego, czy można je traktować jako wiarygodne. Dziękuję za pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Kto z państwa?
Senator Wadim Tyszkiewicz. Bardzo proszę.

SENATOR
WADIM TYSZKIEWICZ

Panie Przewodniczący! Szanowni Eksperci!

Mam pytanie: czy informacje, no, dane pozyskiwane za pośrednictwem Pegasusa mogą znaleźć się w posiadaniu innych, obcych państw, np. poprzez chmurę, serwery? Czy te informacje mogą być przechowywane na serwerach właściciela oprogramowania, w tym przypadku właściciela Pegasusa, czyli firmy NSO? Czyli: telefon – NSO – służby. Czy te informacje trafiają do służb bez pośrednictwa operatora, w tym wypadku Pegasusa? To jest pierwsze pytanie, za chwilę drugie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo proszę panów o odpowiedź.

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. To, co wiemy o sposobie, w jaki Pegasus odsyła informacje, to jest to, że informacje te przechodzą przez serwery, które są wynajmowane w chmurze, od popularnych operatorów chmur, takich jak Amazon. I, jak sądzimy, te serwery są wynajmowane przez samą NSO Group. Ostatecznym odbiorcą informacji, z pewnością jednym z ostatecznych odbiorców tych informacji, jest agencja rządowa, która obsługuje oprogramowanie szpiegujące. Wiemy więc, że informacje te trafiają właśnie tam. Nie mamy jednak pewności, czy informacje nie trafiają także gdzieś indziej. Bardzo trudno mieć co do tego całkowitą pewność, ponieważ uważamy, że serwery są rejestrowane przez samą NSO Group. Nie jest więc jasne, co dokładnie dzieje się poza przekazywaniem informacji operatorowi oprogramowania szpiegującego. Pozostawia to zatem otwarte możliwości i rodzi pytanie: czy informacje te trafiają gdzieś indziej poza operatorem rządowym? Myślę, że jest to możliwość, o którą należy zapytać, należy zadać takie pytanie. Dziękuję.

(*Senator Wadim Tyszkiewicz*: Mogę dopytać?)

Bardzo proszę, Panie Senatorze.

SENATOR
WADIM TYSZKIEWICZ

Czy znacie państwo, panowie, inne, podobne programy służące do inwigilacji? I czy Pegasus istotnie różni się od tych innych programów? Jeżeli tak, to jakie to są różnice? To jest pierwsze pytanie.

I szybko drugie, krótkie. Wśród polskich informatyków krąży informacja, plotka, że część kodu źródłowego jest napisana po chińsku. Jeżeli spotkaliście się panowie z takim przypadkiem, to o czym to może świadczyć, jeżeli to jest prawda? Dziękuję.

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. Co do odpowiedzi na pierwszą część pytania, dotyczącą różnic między Pegasusem a innymi produktami szpiegującymi, to myślę, że najistotniejsza różnica, jaką zaobserwowaliśmy w przypadku Pegasusa w porównaniu do innych produktów tego typu, polega na tym, że posiada on funkcję włamywania się do telefonów za pomocą tzw. exploita *zero-click*. Wszyscy wiemy o potencjale złośliwych linków lub złośliwych plików, o tym, że złośliwe załączniki mogą być wykorzystane jako wektor do dostarczenia oprogramowania szpiegującego. I jeśli użytkownik otworzy złośliwy załącznik lub kliknie w złośliwy link, może nastąpić atak. Jednak metoda *zero-click* nie wymaga absolutnie żadnego działania ze strony celu ataku lub ofiary. *Zero-click* wykorzystuje lukę w aplikacji służącej do obsługi wiadomości, aby automatycznie aktywować się na urządzeniu. Jest to istotna różnica między Pegasusem a innymi rodzajami oprogramowania szpiegującego. Pegasus posiada funkcję *zero-click*, podczas gdy w innych badanych przez nas typach oprogramowania szpiegującego, które, jak się wydaje, są dostarczane głównie za pośrednictwem złośliwych linków lub złośliwych załączników, nie udokumentowaliśmy jeszcze takiej możliwości.

Jeśli chodzi o drugą część pańskiego pytania, to widzieliśmy, że w mediach społecznościowych pojawiły się pewne dyskusje na temat – w cudzysłowie – chińskiego kodu źródłowego Pegasusa. Ale w naszej ocenie wypowiedzi w mediach społecznościowych na ten temat są nieco nietrafne pod względem technicznym i odzwierciedlają niezrozumienie tego, co było przedmiotem analizy. Możemy powołać się tu na to, że w 2016 r. przeprowadziliśmy analizę z firmą Lookout, zajmującą się bezpieczeństwem cybernetycznym, w ramach czego udało nam się uzyskać kopię oprogramowania szpiegującego Pegasus i firma Lookout sporządziła bardzo dokładną, myślę, że blisko 40-stronicową analizę techniczną tego oprogramowania szpiegującego i nie znalazła żadnych elementów wskazujących na istnienie chińskiego kodu źródłowego ani niczego podobnego. Uważam, że jest to wiarygodna analiza techniczna Pegasusa.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Pan senator Michał Kamiński.

SENATOR
MICHAŁ KAMIŃSKI

Jak rozumiem, państwo dzisiaj po raz pierwszy powiedzieli publicznie, że zyskaliście kryminalistyczne dowody na to, że atak bronią cybernetyczną na pana senatora Brejzę miał podtekst polityczny. I, jak rozumiem – jeżeli dobrze zrozumiałem państwa wypowiedź – to rzeczywiście po raz pierwszy pada w polskiej przestrzeni publicznej jako tak sformułowany zarzut i niewątpliwie będzie dla nas źródłem dodatkowej refleksji.

Chciałem, aby pan rozwinął, jeżeli pan może, wątek, który, szczerze mówiąc, również jest nowy w pana wypowiedzi i który również powoduje, no, poważne zaniepokojenie. Mianowicie, jeśli dobrze zrozumiałem, pan dostrzega bezpośrednie analogie metodologiczne pomiędzy działaniami reżimu rosyjskiego przeciwko swoim oponentom a tym, co spotkało pana senatora Brejzę, gdzie prawdopodobnie ta broń została użyta do manipulowania treściami na jego urządzeniach elektronicznych. Czy pan może potwierdzić tę analogię metodologiczną pomiędzy metodami zwalczania cybernetycznego opozycji w Rosji a w Polsce?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za to pytanie. Przede wszystkim muszę powiedzieć, że ustalenie, jaki był konkretny cel zhakowania urządzenia senatora Brejzy i kradzieży jego danych, pozostawimy, jak myślę, państwu i innym kompetentnym organom.

Jeśli chodzi o podobieństwa do działań rosyjskich, to w przypadku służb bezpieczeństwa nie jest niczym wyjątkowym, a już na pewno nie jest to niepowtarzalne w ujęciu historycznym, że pobierają one informacje uzyskane w tajemnicy, manipulują nimi i udostępniają je w jakimś innym celu. Mówimy tu nie o konkretnym działaniu technicznym, ale raczej o procedurze, jak również o usiłowaniu zdyskredytowania danej osoby. Powiedziałbym, że najbardziej przypomina mi to przypadek z opublikowanego przez nas raportu, który nosił tytuł „Tainted Leaks" – „Skażone przecieki" – ponieważ opisane tam było to, w jaki sposób rosyjskie służby pozyskiwały prawdziwe informacje, modyfikowały je i wstawiały tam pewne fałszywe elementy, aby informacje te wywoływały zupełnie inne wrażenie i aby ostatecznie zdyskredytować daną osobę. W tym przypadku usiłowano zdyskredytować Aleksieja Nawalnego.

W ogóle gdy chodzi o takie przypadki, interesujące jest to, że Pegasus zapewnia tak pełny, tak nieograniczony dostęp do świata i życia danej osoby, że zawsze znajdą się materiały, którymi można będzie manipulować i wykorzystać je do wyrządzenia szkody tej osobie. Wszyscy wiemy o długiej i mrocznej przeszłości służb bezpieczeństwa byłego bloku sowieckiego, które wykorzystywały dogłębny dostęp do prywatnego życia i świata ludzi, by im szkodzić. Myślę, że wielu z nas także przypomina sobie o takich przypadkach, gdy patrzymy na przypadek senatora Brejzy. Bardzo dziękuję za to pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo dziękuję.
Pani marszałek Gabriela Morawska-Stanecka.

SENATOR
GABRIELA MORAWSKA-STANECKA

Bardzo dziękuję, Panie Przewodniczący.
Pan we wstępnej części swojej wypowiedzi powiedział, że państwo prowadzili wiele postępowań na całym świecie i jeden klient o jednej nazwie zwrócił państwa uwagę. Czy ta nazwa to „Orzeł Biały"? Jeżeli tak, to czym on się wyróżniał, że zwrócił uwagę? I na jakim obszarze działał?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Pani Senator. To, co widzieliśmy w przypadku tego operatora, wskazywało na to, iż szpiegował wyłącznie na terenie Polski, nie w żadnym innym kraju. A gdy w naszych badaniach widzimy operatora, który szpieguje tylko w jednym kraju, a nie w żadnym innym, to zdecydowanie zwiększa to prawdopodobieństwo, że jest to operator krajowy. Alternatywną odpowiedzią w tym przypadku byłoby to, że Pegasusa kupił jakiś obcy, zagraniczny rząd, ale jeśli kupił go obcy rząd, to dlaczego miałby go używać tylko w jednym kraju poza swoimi granicami, a nie we własnym kraju lub w innych krajach? Dlatego gdy widzimy taki przypadek, że operator szpieguje wyłącznie w jednym kraju, w tym przypadku w Polsce, to zdecydowanie każe nam to sądzić, że jest to operator krajowy, działający lokalnie w danym kraju.

SENATOR
GABRIELA MORAWSKA-STANECKA

To ja mam pytanie: czy on się faktycznie nazywał „Orzeł Biały"? Czy to o tego operatora chodzi?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Tak. Dziękuję, Pani Senator, za pytanie. To był rzeczywiście ten operator.

SENATOR
GABRIELA MORAWSKA-STANECKA

W takim razie mam jeszcze jedno pytanie. Czy w innych przypadkach, kiedy państwo badali setki, tysiące innych operatorów, czy oni też w taki sposób działali? Czy to jest jakieś dziwne, czy inne właśnie, że te działania były prowadzone jedynie na terenie własnego kraju?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję, Pani Senator, za pytanie. W kilku przypadkach zaobserwowaliśmy operatorów działających na terenie własnego kraju. Jak wynika z naszego rozeznania co do licencji tego oprogramowania szpiegującego, zawsze, gdy agencja rządowa kupuje oprogramowanie szpiegujące, nie tylko dostaje określoną liczbę równoczesnych licencji, która ogranicza liczbę celów możliwych do monitorowania w tym samym czasie, ale także ma określany zakres, zasięg geograficzny działania czy też ograniczenie geograficzne. Innymi słowy, domyślny pakiet obejmuje, jak rozumiemy, to, że rząd może szpiegować daną liczbę celów we własnym kraju, a do tego może dopłacić kolejną sumę za zakup licencji na szpiegowanie w innych krajach, za granicą. Tak więc widzimy, że niektórzy klienci szpiegują tylko w granicach swojego kraju, podczas gdy inni, zwłaszcza agencje wywiadowcze, mogą zakupić licencje na szpiegowanie poza granicami. Jednak o tym omawianym tu operatorze możemy powiedzieć, że szpiegował tylko i wyłącznie w Polsce, wyłącznie na terenie własnego kraju. I na to składała się masa obserwacji, to stanowiło całość inwigilacji, jakie widzieliśmy w Polsce. Myślę też, że ciekawą sprawą dotyczącą tego polskiego operatora jest to, że po raz pierwszy aktywność jego infrastruktury odnotowaliśmy dokładnie w listopadzie 2017 r.

PRZEWODNICZĄCY
MARCIN BOSACKI

W listopadzie 2019 r.? To... Chyba wcześniej, no bo jeśli mówicie państwo o senatorze Brejzie, to cały 2019... To znaczy pół roku wcześniej, w 2019 r...

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Być może nastąpił błąd w tłumaczeniu symultanicznym. Powiedzieliśmy o listopadzie 2017 r. To przed chwilą powiedział mój kolega Bill. 2017.

PRZEWODNICZĄCY
MARCIN BOSACKI

To jest bardzo ciekawe, bo z ujawnionych przez Najwyższą Izbę Kontroli 3 dni temu dokumentów wynika – my będziemy mieli zarówno obecnego, jak i byłego prezesa Najwyższej Izby Kontroli przed komisją jutro, i to też jest informacja dla wszystkich państwa – wynika, że prawdopodobny zakup Pegasusa nastąpił pod koniec września 2017 r. Czyli państwo mówicie, że początek działania operatora „Orzeł Biały" w Polsce to jest mniej więcej miesiąc, półtora miesiąca później, w listopadzie 2017 r. Tak?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję, Panie Senatorze, za pytanie. Zgadza się. Pierwsze zaobserwowane przez nas sygnały działalności tego operatora... Co przez to rozumiemy? W tym przypadku to były niektóre serwery, strony internetowe, które były wykorzystywane jako część infrastruktury tego operatora, a dostrzegliśmy je w listopadzie 2017 r., kiedy zostały one po raz pierwszy zarejestrowane. Jest więc całkiem możliwe, że ataki mogły rozpocząć się mniej więcej wtedy lub jakiś czas po tym. Jest to zgodne z tym, co wiemy o tym, jak Pegasus jest uruchamiany i wdrażany po zakupie. Po podpisaniu umowy następuje faza konfiguracji, faza testów, NSO szkoli operatorów w zakresie obsługi, a wszystkie te kolejne kroki wymagają pewnej infrastruktury, pewnego rodzaju serwerów i stron internetowych, by zostało to zarejestrowane i uruchomione.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję.

Ja, za pozwoleniem szanownych kolegów z komisji, pozwolę sobie teraz dopytać paroma pytaniami panów.

Czy ja dobrze rozumiem, że jeśli chodzi o najczęstszy model operowania Pegasusem, przynajmniej w krajach demokratycznych – podkreślam: demokratycznych – to zakupuje je... zakupują Pegasusa struktury państwa, prawdopodobnie wywiady, po to, aby używać Pegasusa poza granicami swojego kraju. Np. Pegasus, jak rozumiem, ma takie możliwości, czyli po to go stworzono, że telefon można zaprogramować i jeśli dana służba wywiadowcza wie, że grupa terrorystów spotyka się, nie wiem, w przyszłą środę o 16.00 i że podsłuchiwany telefon będzie na tym spotkaniu, to można go zaprogramować, że w środę o 16.00 mikrofon zostanie uruchomiony. Czy tak?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za pytanie. Rzeczywiście, powiedziałbym, że materiały marketingowe i publiczne oświadczenia NSO Group, a także niektórych ich klientów wskazują, że jest to narzędzie używane do śledzenia przestępców i terrorystów. I z pewnością ten fenomen, że jest możliwe włączenie mikrofonu podczas spotkania o charakterze poufnym, może być jednym z przykładów jego zdolności. Innym przykładem może być monitorowanie zaszyfrowanych wiadomości danej osoby, nie dlatego, że Pegasus hakuje WhatsApp czy Signal, lecz raczej dlatego, że mając dostęp do urządzenia danej osoby, ma się dostęp do całej prowadzonej przez nią komunikacji. To jest jedna strona tego. To, co jest tak niepokojące w tym przypadku, to jest to, że wchodzi tu w grę bardzo potężny potencjał, chociaż, jak widzimy, senator Brejza wyraźnie nie pasuje do kategorii, które są publicznie określane jako powody użycia Pegasusa.

PRZEWODNICZĄCY
MARCIN BOSACKI

Czyli, dopowiadając: rozumiem, że niewłaściwe użycie Pegasusa, i być może z tym wiąże się odebranie wielu krajom licencji, w tym, jeśli chodzi – proszę potwierdzić – o naszą wiedzę, w Europie, czy w Unii Europejskiej, tylko Polsce i Węgrom, polega na tym, że włącza się system Pegasus w środę o 16.00 nie po to, aby słuchać grupy terrorystów, tylko żeby słuchać posiedzenia sztabu wyborczego na przykład. Tak? I to jest uznawane za niewłaściwe, niezgodne z licencją używanie tego systemu?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Senatorze, za pytanie. Rzeczywiście, wg materiałów NSO... Materiały umowne pomiędzy NSO a klientem wymagają od klienta, jak wierzymy, oświadczenia, że wykorzysta on program do zgodnego z prawem egzekwowania prawa. I wg tych warunków to, o czym pan mówi, z pewnością byłoby użyciem niewłaściwym. Myślę, że generalnie jesteśmy sceptycznie nastawieni do niektórych oświadczeń firmy NSO mówiących o tym, czego wymaga, co mają zrobić jej klienci, jakie są jej własne procedury w zakresie należytej staranności, ale z pewnością taki przypadek mógłby zostać uznany za przypadek nadużycia.

Co do kwestii odcinania klientów, to chciałbym zaznaczyć, że w przeszłości firma NSO składała budzące wątpliwości oświadczenia na temat działań, jakie podjęto lub jakich nie podjęto po ujawnieniu nadużyć. I myślę, że wciąż wielu rzeczy nie wiemy o szczegółach konkretnych działań, które NSO mogła podjąć w stosunku do klientów europejskich. Ale z pewnością... Wspomniał pan o Węgrzech. To kolejny przypadek kraju, w którym zarówno my zidentyfikowaliśmy, jak i badacze Amnesty International, wyraźne przypadki nadużyć co do celów ataków – np. hakowanie dziennikarzy i przedstawicieli mediów.

PRZEWODNICZĄCY
MARCIN BOSACKI

Ostatnie pytanie ode mnie w tej serii. Czy państwo potwierdzacie, że NSO wycofało licencję, czyli możliwość używania Pegasusa, wobec sporej liczby krajów? Jeśli tak, czy były wśród

nich Polska i Węgry? Czy też jest to dla was fakt nieznany i są to tylko wiadomości medialne?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję za pytanie, Panie Senatorze. Nie jesteśmy w stanie potwierdzić działań, jakie firma NSO mogła podjąć lub nie podjęła, chciałbym jednak tylko zaznaczyć, że moim zdaniem oświadczenia NSO o wycofaniu licencji dotyczą zezwoleń na sprzedaż i konkretnych krajów, przy czym nawet w odniesieniu do tego mogą być, jak uważamy, jakieś wyjątki. Mimo wszystko jesteśmy równie ciekawi jak państwo, jakie kroki firma NSO mogła podjąć w stosunku do Polski i polskiego wykorzystania Pegasusa.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Senator Magdalena Kochan.

SENATOR
MAGDALENA KOCHAN

Rozumiem, że instytut, który bada bezpieczeństwo w sieci i odkrył coś, co miało być absolutnie niewykrywalne, czyli działanie Pegasusa, nie do końca chce odpowiadać na pytanie, komu cofnięto lub komu nie cofnięto licencji. Ale moje pytanie dotyczy jeszcze wcześniejszego wątku poruszanego w pytaniach do panów. Mianowicie licencja pozwala na to, żeby jednocześnie inwigilować 10–12 osób. Pierwsze pytanie: czy taka długość inwigilacji – rok, dwa, miesiąc, 2 tygodnie – jest wpisana w tę licencję? Czyli, inaczej mówiąc: czy licencję kupuje się na określony czas, państwo kupuje to na rok, na 2 lata, na 3 lata? To pierwsze pytanie.

A drugie: czy państwo, wiedząc o tym, że nietypowy jak na inne kraje operator o ciekawej nazwie „Orzeł Biały" inwigiluje wyłącznie swoich obywateli, sprawdziliście, że inwigiluje polityka i 2 prawników? Czy wiecie, kogo w tym czasie także podsłuchiwano? Czyli 12 minus 3 osoby, o których wiemy. Czy wiecie, jakie to są inne osoby? Dziękuję.

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Pani Senator. Przede wszystkim nasze stanowisko w kwestii komentowania działań NSO jest takie, że możemy mówić o tym, co widzimy i czemu możemy ufać. A w przypadku działań i oświadczeń NSO nie zawsze możemy zobaczyć, co ta firma robi, i nie zawsze możemy ufać temu, co mówi.

W odniesieniu do licencjonowania nie wiemy, czy licencje Pegasusa w niektórych krajach obejmują prowadzenie obserwacji przez krótki okres, np. 6 lub 12 godzin, a inne licencje pozwalają na znacznie bardziej rozszerzony monitoring. Z pewnością informacje zawarte w umowie z operatorem Pegasusa mogłyby dostarczyć odpowiedzi na te pytania.

Jeśli chodzi o inne osoby w Polsce, których urządzenia mogły zostać zhakowane lub które mogły zostać objęte inwigilacją poprzez Pegasusa, powiedziałbym, że jest to bardzo ważne pytanie i myślę, że to ten konkretny operator Pegasusa, o którym mówiliśmy, byłby w stanie powiedzieć nam wszystkim, kto jeszcze mógł być inwigilowany. Sądzimy, że Pegasus w jego konkretnym wdrożeniu prowadzi klarowny log, rejestr osób, które stały się celem ataku, a być może także tego, jakie dane zostały zebrane. Tego typu rejestr byłby niezwykle pomocny w dochodzeniach takich jak to.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję.
Senator Sławomir Rybicki.

SENATOR
SŁAWOMIR RYBICKI

Dziękuję, Panie Przewodniczący.

Chciałbym zapytać, czy państwo macie wiedzę o praktyce zakupu programu Pegasus. Bo w Polsce jesteśmy świadkami procesu, w którym władza publiczna, a taką jest Ministerstwo Sprawiedliwości i służby specjalne, robiła to w sposób nietransparentny – mogę powiedzieć więcej: w taki sposób, aby ukryć fakt zakupu tego oprogramowania. Użyły do tego pośrednika, firmy Matic, która notabene, o czym donoszą dzisiejsze publikacje, jest firmą prowadzoną przez funkcjonariuszy aparatu bezpieczeństwa w czasach komunistycznych. Czy to jest normalna praktyka, że władze publiczne innych państw próbują zakamuflować zakup urządzenia o nazwie Pegasus? I czy cofnięcie licencji według państwa też przechodziło za pośrednictwem firmy Matic, czy trafiło bezpośrednio do służb? I czy można pod określeniem „Orzeł Biały" jako operatora domniemywać, że to jest jedna ze służb polskich, konkretnie CBA, czy też może się kryć pod tym jeszcze jakaś służba, np. Agencja Wywiadu? Dziękuję bardzo.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze. Odpowiedź na pierwsze pytanie: mamy, można powiedzieć, niedoskonały całościowy obraz procesu zawierania przez NSO umów w sprawie Pegasusa. Jednak w wielu przypadkach dostrzegliśmy dowody na tworzenie firm fasadowych lub przykrywek w celu zakamuflowania ustaleń umownych. Chciałbym zaznaczyć, że w co najmniej jednym znanym nam przypadku okazało się, iż takie dodatkowe ustalenia kamuflowały również pewien stopień urzędniczej korupcji i malwersacji. Ta praktyka wykorzystywania dodatkowych osłon, by zakamuflować transakcje, w kontekście tajności służb specjalnych jest niezwykle ryzykowna właśnie przez wzgląd na korupcję urzędniczą i nadużycia, powoduje też sporo dodatkowych problemów takich jak te, z którymi zmaga się państwa komisja, próbując zrozumieć, co mogło się wydarzyć. Ogólnie rzecz biorąc, w krajach demokratycznych korzystanie przez służby bezpieczeństwa z zasłon w postaci firm fasadowych czy przykrywek jest niezwykle ryzykowne, po prostu dlatego, że w ten sposób można zakamuflować wiele różnych działań, ponadto stworzyć okazje do czerpania korzyści, a obie te sprawy są niezwykle niepokojące.

Odnosząc się konkretnie do sytuacji z Pegasusem w Polsce, powiedziałbym, że naszym zdaniem w Polsce jest prawdopodobnie tylko jeden operator Pegasusa, a przynajmniej był tylko jeden operator. Nie jesteśmy w stanie powiedzieć, który podmiot według nas może być bezpośrednio odpowiedzialny w tej sprawie, ale myślę, że na podstawie wielu poszlak, a teraz też na podstawie tych publicznych stwierdzeń dotyczących umów, możemy rzeczywiście powiedzieć – potwierdzić prawdopodobieństwo – że jest jeden operator Pegasusa. Z uwagi na np. czas rejestracji i inne cechy operatorem tym może być rzeczywiście „Orzeł Biały". Mam nadzieję, że ta komisja będzie mogła dokładniej to zbadać i ustalić fakty dzięki innym składanym tu zeznaniom.

Zaznaczę jeszcze, że gdy przyglądamy się sprawie polskiej, to dostrzegamy wiele elementów znanych z innych spraw użyć Pegasusa gdzieś indziej w świecie, np. wykorzystywanie firm fasadowych, zawsze jednak niepokoi nas, gdy widzimy takie przypadki w kraju demokratycznym. Tak więc wyzwania, które każdy teraz może dostrzec, tworzą się po to, by zrozumieć, co dokładnie się stało, oraz zapewnić odpowiedzialność za to.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Pan marszałek, senator Michał Kamiński. Bardzo proszę o zadanie pytania.

SENATOR
MICHAŁ KAMIŃSKI

Ja mam pytanie. Czy panowie są w stanie w przyszłości, w toku dalszych badań, ustalić głębsze szczegóły ataków na te osoby, które nas interesują, czyli na panią prokurator Wrzosek, na pana mecenasa Giertycha i na pana senatora Brejzę? Co mam na myśli, mówiąc „szczegóły ataków"? To znaczy: czy są państwo w stanie technicznie, kiedyś, w przyszłości, ustalić, jakie informacje były przedmiotem ataku tego, kto

atakował, na np. telefonie bądź innych nośnikach pana senatora Brejzy, a także jakich ewentualnie manipulacji tam dokonano? To znaczy czy oprócz tego generalnego śladu ataku państwo są w stanie rozpracować szczegóły poszczególnych ataków Pegasusem?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. W niektórych przypadkach udaje nam się zidentyfikować rodzaje informacji, które zostały pobrane, rzadko jednak z taką dokładnością, by określić np. pojedyncze zdjęcia lub pojedyncze pliki. Ale czasami, po przeprowadzeniu śledztwa, możemy zrozumieć, jaka funkcja Pegasusa mogła zostać aktywowana – np. funkcja mikrofonu, funkcja kamery lub funkcja robienia zdjęć. Tak więc jest możliwe, że dzięki dodatkowemu śledztwu i dodatkowej analizie będziemy w stanie ustalić jakieś szczegóły dotyczące rodzajów aktywowanych funkcji. Kontynuujemy badania, analizujemy każdy z tych przypadków i spodziewamy się, że będziemy w stanie powiedzieć więcej na temat tego, co konkretnie zostało aktywowane i co mogło zostać pobrane, będzie to jednak wymagało dalszego dochodzenia, i my obecnie je prowadzimy.

SENATOR
MICHAŁ KAMIŃSKI

Mówiąc inaczej: my mamy szansę dowiedzieć się, jakie były szczegóły tego ataku, a tym samym będziemy mogli się przekonać, czy rzeczywiście motywy tych, którzy atakowali, były motywami dotyczącymi walki z przestępczością, czy miały zupełnie inny charakter?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, odpowiadając na to pytanie, zaznaczę, że generalnie na podstawie dowodów kryminalistycznych byliśmy w stanie określić takie kwestie jak czas i aktywność. Jeśli jednak próbowalibyśmy odpowiedzieć na pytanie, czy ukierunkowanie ataku było motywowane politycznie, to cóż... My mamy istotne dowody poszlakowe co do czasu, kradzieży informacji i śladów infekcji. Zachęcam pana senatora i pańskich kolegów do próby uzyskania informacji o logach od polskiego operatora Pegasusa, bo one mogą zawierać istotne potwierdzenia konkretnych działań, a być może także wskazywać bezpośrednio na pewne motywacje i łańcuch poleceń, co doprowadziłoby do kwestii obrania za cel konkretnych osób w konkretnym czasie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Pani senator Gabriela Morawska-Stanecka.

SENATOR
GABRIELA MORAWSKA-STANECKA

Bardzo dziękuję.
Ja mam jeszcze pytanie takie odnośnie zasady działania tego Pegasusa. Czy ten operator Pegasusa, kiedy zainfekuje urządzenie, telefon w tym wypadku, ma dostęp do takich wiadomości, które użytkownik tego telefonu posiada w chmurze, czyli nie na urządzeniu, ale w chmurze, i czy może się zapoznać z treścią tych wiadomości, jeżeli ten operator Pegasusa ma taką potrzebę? To jest pierwsze pytanie, chciałabym uzyskać na nie odpowiedź.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Pani Senator, uważamy, że to prawda, uważamy także, że dostęp do chmury może być utrzymywany po zakończeniu infekowania danego urządzenia. Uważamy, że Pegasus może wykraść tokeny dostępu używane przez telefon do uwierzytelniania się w usługach chmurowych i z powodzeniem stworzyć duplikat kluczy

danej osoby do jej środowiska w chmurze oraz wszystkich znajdujących się tam rzeczy. To również jest niesamowicie inwazyjne i może być długotrwałe.

(*Senator Gabriela Morawska-Stanecka*: Jeszcze jedno mogę?)

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo proszę, Pani Marszałek.

SENATOR
GABRIELA MORAWSKA-STANECKA

Mam jeszcze pytanie takie: czy ten operator „Orzeł Biały" na podstawie państwa informacji – bo już usłyszeliśmy tutaj, że ta pierwsza aktywność była pod koniec 2017 r... Czy na podstawie wiedzy, jaką państwo zgromadziliście, możecie oszacować, że to narzędzie było stosowane w większej skali, czyli wobec innych osób niż tylko te trzy, o których już wiemy, że zostały zaatakowane tym systemem?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Cóż, widzieliśmy dowody innych infekcji. Na podstawie naszych technik skanowania sieci uważamy, że mogą one nie być związane z tymi wspomnianymi osobami, dlatego sądzę, że tak ważne jest prowadzenie dalszego dochodzenia w tej sprawie. Ogólnie rzecz biorąc, można powiedzieć, że w tym przypadku spodziewalibyśmy się, że są inne ofiary. Oczywiście wyzwaniem jest ustalenie, kim one są i co mogło zostać pobrane. Jeszcze raz dziękuję za pytanie, Pani Senator.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Senator Jacek Bury, bardzo proszę.

SENATOR
JACEK BURY

Chciałem zapytać, czy... Bo rozumiem, że mamy tutaj potwierdzone przypadki ingerencji za pomocą systemu iOS iPhone firmy Apple. A czy ten system Pegasus jest w stanie infekować też telefony, które bazują na innych systemach operacyjnych, takich jak Android? I czy poprzez telefony – albo nie tylko poprzez telefony – Pegasus jest w stanie inwigilować i wpływać na zawartość, szpiegować zawartość np. laptopów, które są zsieciowane?

STARSZY PRACOWNIK NAUKOWY W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. Uważamy, że Pegasus ma funkcjonalność dotyczącą systemu Android, innymi słowy, może infekować nie tylko iPhone'y, ale może także infekować i inwigilować urządzenia z systemem Android. Jeśli chodzi o wykorzystanie Pegasusa w przypadku urządzeń, które nie są telefonami komórkowymi, to według naszego rozeznania Pegasus jest systemem przeznaczonym wyłącznie do inwigilacji telefonów komórkowych. Jednak informacje zebrane z telefonu na temat sieci – np. jeśli telefon i inne urządzenia znajdują się w tej samej sieci – mogą zostać wykorzystane jako wstęp do innych ataków lub innych operacji szpiegowskich z użyciem innego rodzaju narzędzi. Niemniej jednak z tego, co wiemy, Pegasus jako narzędzie samo w sobie jest zaprojektowany wyłącznie z myślą o telefonach, iOS, Android. Mówi się także o tym, że inne linie telefonów, takie jak BlackBerry czy starsze smartfony Nokii, też mogą być celem ataków z użyciem Pegasusa.

SENATOR
JACEK BURY

Jeszcze jedno pytanie mam. Jeżeli chodzi o senatora Brejzę, to mieliśmy podaną ilość ataków, natomiast ciekaw jestem, jak intensywne były ataki na mecenasa Giertycha czy panią prokurator Wrzosek. Czy są w stanie panowie przybliżyć skalę tych ataków?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za pytanie. Sięgnę do swoich notatek i wkrótce udzielę odpowiedzi. Wydaje mi się, że co do przypadku mecenasa Giertycha, to podał on do publicznej wiadomości liczbę ataków. Nie mam pewności, czy zrobiła to prokurator Wrzosek. Zasadniczo polityka Citizen Lab zakłada niekomentowanie spraw bez zgody osoby, której one dotyczą.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Senator Wadim Tyszkiewicz. Bardzo proszę.

SENATOR
WADIM TYSZKIEWICZ

Mam pytanie. Czy znacie państwo przypadki postępowań sądowych wytoczonych przez obywateli służbom inwigilującym? Oczywiście mówimy o krajach demokratycznych, bo w niedemokratycznych takie postępowania nie mają sensu. Czy znacie takie przypadki, że obywatel wytoczył proces za inwigilowanie go właśnie tym narzędziem? Z jakim rezultatem? To jest pierwsze pytanie.

I mnie jeszcze dręczy pytanie, że skoro można zmanipulować praktycznie wszystko, co się znajduje na telefonie, czy taki dowód z w ten sposób pozyskanych informacji może być użyty w procesie sądowym jako dowód – skoro można manipulować tymi danymi, można do telefonu dopisać coś, czego ktoś nie zrobił, albo przypisać komuś działania, które nie były jego udziałem. Więc skoro można manipulować danymi w telefonie, czy takie dane z tego telefonu mogą być dowodem w sprawie?

I takie dosyć przewrotne pytanie. Skoro Pegasus był sprzedawany w roku 2016 czy 2017 jako oprogramowanie niewykrywalne, a polski rząd za pomocą służb wydał trzydzieści kilka milionów złotych na to oprogramowanie, to czy teraz służby specjalne Polski nie powinny zażądać zwrotu tych pieniędzy, skoro jednak to oprogramowanie jest wykrywalne, czyli w pewnym sensie jest wadliwe.

I już ostatnie pytanie...
(*Przewodniczący Marcin Bosacki*: Nie...)
Okej, dobrze. Dziękuję.

PRZEWODNICZĄCY
MARCIN BOSACKI

Nie za dużo na raz, nie za dużo na raz, Panie Senatorze, za chwilę panu oddam jeszcze raz głos.

Bardzo proszę, Panowie, o odpowiedź.

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za pytania. Po pierwsze, jesteśmy świadomi licznych spraw wynikających z nadużyć NSO, są to sprawy dotyczące kilku różnych lokalizacji. Są nam znane przypadki osób, które wniosły pozwy przeciwko NSO Group, w niektórych przypadkach mogą to być także sprawy przeciwko rządom. Obserwujemy też rosnącą liczbę przypadków, w których duże firmy technologiczne pozywają NSO Group – dotyczy to zarówno WhatsApp, jak i Facebooka oraz Apple. A w przypadku pozwu wniesionego w 2019 r. przez WhatsApp i Facebooka wiele innych dużych firm technologicznych, w tym Google i Microsoft, dołączyło do nich w ramach tzw. instytucji *amicus brief*, by wesprzeć ten pozew.

Co do kwestii dowodów pochodzących z urządzenia z Pegasusem, to powiedzielibyśmy, że jest to owoc zatrutego drzewa. Bo po tym, jak już włamano się do urządzenia w ten niezwykle inwazyjny sposób, jaka może być gwarancja, że nie dokonano tam modyfikacji lub manipulacji? Domyślam się, że wytrawny prokurator czy obrońca byłby w stanie dać bardzo mocny odpór w przypadku dowodów uzyskanych w ten sposób, z uwagi na inwazyjność i potencjalność modyfikacji materiału znajdującego się w systemie.

Jeśli chodzi o trzecie pańskie pytanie, to, jak rozumiem, brzmi ono: czy polskim służbom

należy się zwrot pieniędzy, gdyż kupiona technologia została wykryta? Myślę, że ogólnie rzecz biorąc to, co wiemy o NSO Group i jej produkcie, sugeruje, iż jeśli służby bezpieczeństwa go nabyły, to być może nie przeprowadziły pełnej analizy dotyczącej możliwości jego wykrycia, a być może także analizy ryzyka dla bezpieczeństwa narodowego w związku z używaniem oprogramowania szpiegującego mającego skomplikowaną infrastrukturę w chmurze, wyprodukowanego przez czołową firmę z innego kraju, która ma powiązania ze służbami bezpieczeństwa tego kraju. Myślę, że są to bardzo ważne pytania, a jeśliby do nabycia tego produktu wykorzystano publiczne pieniądze, to naprawdę pytania w tym kontekście należałoby postawić.

Jeszcze o jednym chciałbym wspomnieć. Otóż nie mam wiedzy, czy NSO udziela gwarancji konkretnie co do tego, że jej oprogramowanie szpiegujące jest niewidzialne, ale z pewnością głoszą oni w domenie publicznej oświadczenia o jego niewykrywalności. To znów jest kwestia, na którą można by odpowiedzieć dzięki dogłębnej analizie materiałów kontraktowych dostarczonych przez NSO oraz wszelkich informacji udzielonych ustnie czy w inny sposób, które mogły zostać przekazane polskim służbom bezpieczeństwa.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Jeszcze...

(*Senator Wadim Tyszkiewicz*: Jeszcze krótkie pytanie chciałem...)

...pytanie senatora Tyszkiewicza. Bardzo proszę.

SENATOR
WADIM TYSZKIEWICZ

Chciałbym uzupełnić pytanie, które wcześniej zadał senator Bury. Bo rzeczywiście Pegasus, z tego, co panowie mówią, nie ma dostępu do komputerów. Ale bardzo często na telefonach mamy programy czy bazy danych, które się powielają z komputerem – tak? Czyli na przykład poczta elektroniczna, która jest też zainstalowana, powiedzmy Gmail, na telefonie. Czyli rozumiem, że poprzez Pegasusa i dostęp do telefonu można uzyskać dostęp do wszystkich programów i danych, które są i na komputerze, i na telefonie zainstalowane. Dziękuję.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, z pewnością telefony – iPhone'y są tego dobrym przykładem – mają w coraz większym stopniu możliwości tzw. bezproblemowego połączenia z komputerem użytkownika, tak więc potencjalnie wiele materiałów znajdujących się na komputerze mogłoby znajdować się też na iPhonie. Co więcej, np. jeśli komputer i iPhone korzystają z iCloud, to, biorąc pod uwagę to, że Pegasus potencjalnie pozwala operatorowi uzyskać zdalny dostęp do iCloud, moglibyśmy zaobserwować coś w rodzaju tylnej furtki, by uzyskać dostęp do materiałów znajdujących się na komputerze. Jeszcze raz dziękuję za pytanie, Panie Senatorze.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję.

Zgodnie z Regulaminem Senatu oczywiście pozostali senatorowie mają prawo zadawać pytania podczas posiedzeń komisji.

Bardzo proszę o zadanie takiego pytania pana senatora Marka Borowskiego.

SENATOR
MAREK BOROWSKI

Dziękuję bardzo, Panie Przewodniczący.

W trakcie dyskusji, która toczyła się w Senacie wtedy, kiedy powoływaliśmy naszą komisję, senatorowie zadawali bardzo wiele pytań. I byli m.in. także senatorowie, którzy wyrażali pewien niepokój, a może nawet pewną podejrzliwość dotyczącą źródeł finasowania waszej instytucji, czyli Citizen Lab. Ja spojrzałem na stronę internetową Citizen Lab, tam są wymienieni sponsorzy, muszę powiedzieć,

bardzo szacowni – są to różnego rodzaju fundacje, zarówno prywatne, jak i publiczne, ale znane. Chciałbym się w związku z tym dowiedzieć, czy ta lista, która jest na stronie internetowej, sponsorów Citizen Lab... Czy to jest lista kompletna, to znaczy poza nią nie ma żadnego znaczącego sponsora?

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za pytanie. Citizen Lab wykonuje swoją pracę już od ok. 20 lat, nasza siedziba znajduje się na Uniwersytecie w Toronto, będącym jednym z najbardziej prestiżowych uniwersytetów w Kanadzie, a wszystkie nasze działania są pod każdym względem niezależne od wpływów rządowych i korporacyjnych. Szczycimy się również tym, że nasza praca jest niezależna od wpływów jakichkolwiek sponsorów. Stanowczo nie bierzemy od fundatorów pieniędzy na konkretne działania śledcze. Ja pracuję w Citizen Lab od 10 lat i nigdy nie spotkałem się z przypadkiem próby ingerencji ze strony sponsora. W ramach naszego nieustannego dążenia do zapewniania przejrzystości staramy się wymieniać wszystkich naszych głównych sponsorów bezpośrednio na naszej stronie internetowej. Nie mogę zagwarantować, że w okresie poprzedzającym moją pracę nie było tam jakichś przeoczeń, ale mogę powiedzieć, że według mojej najlepszej wiedzy ta lista jest poprawna.

Generalnie tego rodzaju praca jest ciekawym wyzwaniem. Kiedy zaczynasz pracę dotyczącą jakiegoś kraju, ktoś zaraz pyta: dlaczego nagle zainteresowałeś się naszym krajem? Odpowiedź jednak jest zawsze taka sama: naszym zadaniem jest badanie zagrożeń hakerskich i cyfrowych dla społeczeństwa obywatelskiego. I nie boimy się zgłaszać takie przypadki, gdziekolwiek je znajdziemy. Chciałbym też zaznaczyć, że Citizen Lab występował jako poważny krytyk polityki inwigilacji również w Kanadzie. Nie ograniczamy się więc do zajmowania się tylko konkretnymi sprawami czy obszarami tematycznymi. Uważamy, że jest to jeden ze sposobów, aby ludzie mogli nam ufać. Dziękuję za pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo proszę, Panie Senatorze.

SENATOR
MAREK BOROWSKI

Rzeczywiście, jedno z głównych waszych pól działalności to są badania nad legalnością działań w zakresie technologii komunikacyjnych, praw człowieka, ingerencji w te prawa człowieka itd. I moje pytanie jest takie: czy zajmujecie się wyłącznie takimi przypadkami właśnie, czy też macie jakiś dział, który zajmuje się, no, np. opracowywaniem pewnych rekomendacji dotyczących tego, jak powinien wyglądać nadzór nad taką działalnością niejawną – a przecież potrzebną, konieczną? Nasza komisja jako jedno z zadań ma opracowanie takiego systemu, to znaczy poprawienie tego, który jest – bo to nie jest tak, że go w ogóle nie ma w Polsce, ale chodzi o poprawienie go – i być może z waszej strony mogłyby być przekazane jakieś rekomendacje, jakieś pomysły w tym zakresie, wynikające z waszych doświadczeń.

PRZEWODNICZĄCY
MARCIN BOSACKI

Popieram sugestię pana senatora. I bardzo proszę o odpowiedź na pytania.

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za pytanie. Na badania i pracę Citizen Lab składają się 3 elementy. Ja zajmuję się prowadzeniem dochodzeń, a 2 inne nasze główne komponenty... Jeden z nich to, jak pan słusznie zauważył, badanie nadzoru nad inwigilacją – i tu w dużej mierze koncentrujemy się na kontekście północnoamerykańskim, ale z pewnością naukę wyciągniętą z tego można stosować w szerszym zakresie. Trzecim komponentem naszej pracy jest śledzenie cenzury

i manipulacji informacjami, czyli badanie cenzury i dezinformacji – tu w większości skupiamy się na Chinach i Rosji, ale pracowaliśmy też nad Iranem i innymi sprawami. Ogólnie rzecz biorąc, uważamy, że częścią wyzwania związanego z nadzorem nad inwigilacją jest świadomość istnienia problemu, ponieważ ten świat jest utajniony celowo. I czasami problem musi stać się naprawdę poważny, żeby pojawiła się choć jakaś publiczna wskazówka, że coś poszło nie tak.

W tym przypadku powiedziałbym, że nasze odczucie jest takie – i być może to jest taka publiczna wskazówka – że rzeczywiście coś poszło bardzo źle. Dlatego z zadowoleniem podejmiemy dalsze rozmowy na temat znaczenia nadzoru nad inwigilacją i modeli nadzoru, które mogły się sprawdzić w przeszłości w innych miejscach i które być może są bardziej problematyczne.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Z całą pewnością zachowujemy sobie prawo rozmawiania z państwem, nie tylko dzisiaj, tylko również później, kiedy będziemy się właśnie zajmowali tą częścią naszej pracy, która ma zaproponować Senatowi, a potem całej Rzeczypospolitej, pewien nowy system nadzoru nad służbami specjalnymi i ich technikami inwigilacji.

Teraz jeszcze mamy kilka pytań, pewnie już ostatnich, ze strony senatorów. Pani senator Magdalena Kochan, potem pan senator Sławomir Rybicki.

SENATOR
MAGDALENA KOCHAN

Bardzo dziękuję, Panie Przewodniczący.

Ja chciałam troszkę nawiązać do tych bardzo szczegółowych, technicznych pytań. Panowie powiedzieliście przed chwilą, że system Pegasus właściwie został stworzony dla inwigilacji telefonów komórkowych. Ale, jak wiemy, telefony służą nam w tej chwili i są połączone i z naszym domowym komputerem, i z tabletem. Pytanie: czy hasła do naszej poczty, które otwieramy w każdym z tych urządzeń, są do wykrycia i poprzez... do zhakowania, i poprzez te hasła mamy pełen dostęp, czy, przepraszam, inwigilujący ma pełen dostęp do naszej korespondencji, nawet tej najbardziej tajnej, jaka jest okryta tajemnicą adwokacką czy tajemnicą śledztwa, tajemnicą lekarską? Czy to jest możliwe technicznie?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Pani Senator, dziękuję za pytanie. Jedną z najtrudniejszych części mojej pracy jest skontaktowanie się z kimś i potwierdzenie, że jego telefon został zainfekowany Pegasusem. Moment poznania tego faktu jest trudny. Potęguje to jeszcze to, że muszę poinformować taką osobę, iż dane uwierzytelniające, których używa w telefonie, aby uzyskać dostęp do usług online, w tym do poczty elektronicznej, również mogły zostać przejęte. Myślę, że nie powinniśmy zapominać o wpływie inwigilacji za pomocą Pegasusa na wymiar osobisty. Ma ona charakter totalny i, jak słusznie pani zauważyła, może obejmować konta internetowe oraz dane uwierzytelniające do tych kont. Chodzi tu o perspektywę osoby, której życie, podobnie jak życie każdego z nas, jest mieszanką tego, co jest w naszym umyśle, tego, co mówimy osobiście, i tego, co robimy za pomocą naszych licznych urządzeń. A Pegasus tak bardzo, jak to tylko możliwe, infiltruje ten nasz świat, a także może być wykorzystany, aby obrócić go przeciwko nam. Jest to bardzo złe pod względem psychologicznym, jest to niezmiernie inwazyjne, z technicznego punktu widzenia jest również bardzo inwazyjne.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.
Senator Rybicki.

SENATOR
SŁAWOMIR RYBICKI

Dziękuję.

Chciałbym zapytać pana o rozwinięcie wątku, o którym pan wspomniał, o różnego rodzaju waszych działaniach – zresztą przez publicystów

nazywanych... Pisze się, że jesteście państwo strażnikiem demokracji w internecie. Gdyby zechciał pan powiedzieć o konkretnych śledztwach zakończonych przez państwa w badaniach nad przypadkami w świecie – wiemy o Polsce już dość dużo – o przypadkach badania działalności Pegasusa na Węgrzech i w innych państwach świata, które zakończyły się realizacją, czyli wykryciem sprawców i w jakich to było sprawach... Prosimy o informacje w tym zakresie.

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję, Panie Senatorze, za pytanie. Było wiele spraw do tego czasu. Jednym z obszarów, o którym możemy powiedzieć, że był to najdłuższy proces śledczy, jest dochodzenie w sprawie nadużyć w związku z Pegasusem w innym kraju demokratycznym, w Meksyku. W tym przypadku zaczęło się od dwóch osób, które, jak stwierdziliśmy, zostały zhakowane, ale ostatecznie ustaliliśmy, że było ich o wiele więcej. Rząd meksykański wszczął w tej sprawie oficjalne dochodzenie i postępowanie karne, które obecnie jest w toku. Dzięki tym wstępnym obserwacjom dowiedzieliśmy się bardzo wiele o rządzie meksykańskim, kliencie, i o nadużywaniu Pegasusa. Istnieje też interesująca analogia: wśród osób, które były celem działań z wykorzystaniem Pegasusa, był szef jednej z wiodących partii opozycyjnych w Meksyku.

Na całym świecie były przypadki, które dostrzegliśmy i z których dowiedzieliśmy się znacznie więcej o wdrożeniach Pegasusa. Zazwyczaj takie przypadki zdarzają się w krajach demokratycznych i w krajach, w których działają prężnie wolne media. Zaznaczę jednak, że w tych przypadkach, z których dowiedzieliśmy się znacznie więcej, nie chodziło o dowody czysto techniczne, ale raczej o postępowanie za pracami innych osób – czy to dziennikarzy śledczych, czy komisji śledczych – czy za dochodzeniami prowadzonymi przez organy prokuratorskie. W sprawie meksykańskiej aresztowano już jedną osobę powiązaną z procesem zawierania umów, z jednej z firm, które brały w tym udział. To pokazuje nam, że aby naprawdę zrozumieć, co się stało, jaki był tego zakres i skala, nie można poprzestać na dowodach technicznych – one rozpoczynają dochodzeniową przeprawę, ale ostatecznie dowody, które są naprawdę znaczące, będą u operatora rządowego i w zeznaniach osób, które prowadziły operacje rządowe.

SENATOR
SŁAWOMIR RYBICKI

Dziękuję bardzo.

Dopytam wobec tego jeszcze. Czy rząd Meksyku w jakikolwiek sposób kwestionował waszą działalność, osiągnięcia badawcze waszego zespołu? Czy kwestionował ustalenia, które poczyniliście? Dziękuję.

STARSZY ANALITYK W THE CITIZEN LAB W MUNK SCHOOL OF GLOBAL AFFAIRS & PUBLIC POLICY NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

To typowe, że kiedy publikujemy raport, to rząd, który może być sprawcą nadużyć, stara się wzbudzić wątpliwości. Robi to na kilka sposobów. Mówi: „Kim są Citizen Lab? Nigdy wcześniej o nich nie słyszeliśmy". Może też próbować mówić tak: „Co to za dowody? Wątpimy w nie". Może nawet wynająć eksperta, który przygotuje wątpliwej jakości dokument techniczny podważający nasze ustalenia. My odpowiadamy na to tak: spójrzcie na to, kto tak nie mówi. A mianowicie są to duże firmy technologiczne. Np. firma Apple dwukrotnie zaktualizowała wszystkie urządzenia Apple na całym świecie właśnie na podstawie ustaleń Citizen Lab dotyczących Pegasusa. Nie robiłaby tego, gdyby te wyniki nie były prawdziwe. Podobne zmiany i aktualizacje zostały wprowadzone przez wiele dużych platform. Ale nie należy na tym poprzestawać. Proszę pamiętać, że w przypadku namierzania senatora Brejzy nie musicie państwo ufać Citizen Lab. Amnesty International, która również prowadzi badania w sprawie oprogramowania szpiegującego, przeprowadziła niezależną analizę materiałów kryminalistycznych w tej sprawie i stwierdziła, że nasze wnioski były trafne. Myślę, że jeśli szukacie dowodów na to, że badania są rzetelne, to można je znaleźć wszędzie.

My przyzwyczailiśmy się już do tego, że zawsze są usiłowania znalezienia czegoś, jakieś próby zdyskredytowania naszych ustaleń.

W przypadku Meksyku oczywiście było początkowe dyskredytowanie, ale oto teraz, po wielu latach, wyraźnie widać, że toczy się tam długotrwałe i dogłębne oficjalne śledztwo. Jesteśmy do tego przyzwyczajeni.

Chciałbym również zaznaczyć – to tylko kolejny przykład – że WhatsApp również wprowadził aktualizacje wszystkich swoich aplikacji klienckich na podstawie ustaleń wynikających z naszych badań. Podobna sytuacja ma miejsce w przypadku Microsoftu w związku z innym oprogramowaniem szpiegującym. Dziękuję za pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję.
Pani marszałek Morawska-Stanecka.

SENATOR
GABRIELA MORAWSKA-STANECKA

Bardzo dziękuję.

Ja jeszcze wróciłabym do tych kwestii technicznych. Mam takie 2 pytania.

Czy... Po pierwsze, jeżeli ten system tak głęboko wnika w telefon, to czy jeżeli za pomocą mojego telefonu steruję alarmem w mieszkaniu, załączaniem, wyłączaniem urządzeń w mieszkaniu, to czy ten system może to samodzielnie robić, łącznie np. z możliwością sabotażu, czyli zdezaktywowanie alarmu albo załączenie jakiegoś ogrzewania, załączenie czegoś w mieszkaniu poza moją wiedzą i wolą? To jest pierwsze pytanie.

I drugie pytanie. Czy jeżeli w trakcie ataku na telefon kogokolwiek – czyli u nas mamy te 3 przypadki: senatora Brejzy, pani prokurator Wrzosek czy pana mecenasa Giertycha – w tym czasie kontaktowały się z tymi osobami inne osoby, to czy wtedy telefony tych osób mogły zostać zainfekowane, czy też nie?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Pani Senator. Ogólna odpowiedź na pierwsze pytanie jest taka, że po tym, jak urządzenie zostało zhakowane za pomocą Pegasusa, jego operator może zrobić w zasadzie wszystko to, co może zrobić użytkownik telefonu. Istnieje więc możliwość otworzenia pewnych aplikacji w telefonie, uruchomienia pewnych funkcji w pewnych aplikacjach na telefonie zainfekowanym Pegasusem. Jest więc z pewnością możliwe... Główną ideą Pegasusa jest to, że daje on operatorowi pełną kontrolę nad urządzeniem, w tym nad aplikacjami i danymi. Tak więc wspomniana przez panią sytuacja rzeczywiście jest możliwa.

Jeśli chodzi o drugie pytanie, dotyczące osób komunikujących się z zainfekowanym urządzeniem, to z pewnością jest możliwe, że po tym, jak telefon został zainfekowany, operator może wykorzystać pewne jego funkcje, np. wysyłać wiadomości wyglądające tak, jakby pochodziły od zaufanego kontaktu, a jeśli te wiadomości są następnie wysyłane do kogoś innego, to mogą one być wykorzystane do przesłania np. złośliwego linku lub złośliwego pliku. Osoba, która je otrzyma, zobaczy, że pochodzą one od kogoś zaufanego, i będzie bardziej skłonna do interakcji lub otwarcia ich. Myślę więc, że jest to jak najbardziej możliwe. Udokumentowaliśmy tego rodzaju funkcjonalność do wysyłania wiadomości do kogoś innego w innych rodzajach oprogramowania szpiegującego, które posiadają funkcję korzystania z konta bezpośrednio na urządzeniu. Jest to więc z pewnością możliwe, gdyż oprogramowanie szpiegujące umożliwia pełną kontrolę i pełne wykorzystanie urządzenia przez operatora oprogramowania szpiegującego.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo dziękuję.

Szanowni Państwo...

(*Starszy Analityk w The Citizen Lab w Munk School of Global Affairs & Public Policy na Uniwersytecie w Toronto John Scott-Railton*: Ja mogę dodać... O, przepraszam bardzo...)

Oczywiście, bardzo proszę.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Gdybym miał urządzenie, którego używałbym np. jako smart locka, inteligentnego zamka

do domu, i dowiedziałbym się, że zostało ono zainfekowane Pegasusem, natychmiast zacząłbym się niepokoić, czy ktoś może się dostać mojego domu, np. otworzyć sobie drzwi.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Szanowni Państwo, wygląda, że mamy jeszcze 3 zgłoszenia i potem będziemy kończyć. Ja jeszcze będę miał pewien apel do szanownych naszych gości dzisiejszych.

Bardzo proszę, marszałek Michał Kamiński.

SENATOR
MICHAŁ KAMIŃSKI

Ja mam 2 sprawy.

Pierwsza. Jak rozumiem, każda z zainteresowanych w Polsce osób może się z państwem kontaktować, aby ustalić, czy padła ofiarą takiego ataku. Rozumiem, że państwo taką możliwość dla różnych obywateli polskich posiadacie. Czy dobrze zrozumiałem?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Dziękuję za to pytanie, Panie Senatorze. Citizen Lab jest nadal bardzo zainteresowane sprawą polską, ale zazwyczaj nie komentujemy publicznie szczegółów naszej metodologii dochodzeniowej. Ogólnie powiedziałbym, że praca Citizen Lab skupia się na kwestiach upoważnień, w tym dotyczących kierowania ataków na społeczeństwa obywatelskie, a w niektórych przypadkach na partie opozycyjne w demokracjach. Poza tym nie mogę powiedzieć zbyt wiele na temat tego, jakie sprawy i w jaki sposób możemy rozpatrywać lub nie możemy. Dziękuję jednak za zrozumienie tej kwestii.

SENATOR
MICHAŁ KAMIŃSKI

Rozumiem.

A ja mam jeszcze jedno pytanie, ponieważ to, co państwo ustalili... Jedną z ofiar tego systemu jest pan mecenas Roman Giertych. W jego przypadku mamy do czynienia z ewidentnym złamaniem tajemnicy adwokackiej – wyciekły jego maile z klientem, które zostały, no, najprawdopodobniej również tym systemem zhakowane. Ale moje pytanie jest generalne: czy z panów wiedzy wynika, że zastosowanie oprogramowania Pegasus do osób, których profesja jest objęta tajemnicą, takich jak np. mecenas, praktycznie uniemożliwia zachowanie tej tajemnicy? To znaczy, że zakres kontroli, jaką ma nad naszym życiem ten system, ta broń elektroniczna, zakres informacji, do jakich ma dostęp, uniemożliwia selektywne wybranie jakiejś informacji, tylko tak naprawdę uniemożliwia jakiekolwiek zachowanie tajemnicy adwokackiej. Czyli ktokolwiek godzi się na użycie Pegasusa wobec mecenasa, zakłada, że tajemnica adwokacka będzie łamana.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, rzeczywiście jest wiele zawodów, które mają taką ochronę prawną, takie uprzywilejowanie. Z pewnością Pegasus nie jest wyznawcą żadnej formy ochrony prawnej i uprzywilejowania, dlatego jest tak niebezpiecznym narzędziem, można bowiem wyobrazić sobie sytuację, w której istnieje ogromna pokusa uzyskania dostępu do komunikacji tego rodzaju. Powiedziałbym, że rzeczywiście jest to powód, dla którego większość konstytucji przewiduje, że taka ochrona ogranicza działania służb bezpieczeństwa. Pegasus zaś cyfrowo usuwa wszelkie ograniczenia.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Dwa ostatnie pytania. Senator Marek Borowski, a potem – bo prosił o możliwość zadania jednego pytania – pan poseł Michał Gramatyka.

SENATOR
MAREK BOROWSKI

W odpowiedzi na pytanie pani senator Morawskiej-Staneckiej powiedział pan, że

jest całkiem możliwe, iż operator, włamując się do cudzego telefonu – ponieważ może się zachowywać tak jak właściciel – może z tego telefonu wysyłać różnego rodzaju informacje złośliwe, jakieś linki itd., itd. No właśnie tutaj ostatnio, w ciągu ostatnich 2 dni, 3 dni, mieliśmy do czynienia, tu u nas, w Polsce, z pewnym dziwnym zjawiskiem, mianowicie z telefonu małżonki pana senatora Brejzy, a także z telefonu córki pana mecenasa, adwokata Giertycha, wysyłane były do różnych instytucji – fałszywe oczywiście – informacje o tym, że podłożona została jakaś bomba, że istnieje jakieś zagrożenie itd., itd. Było to dosyć masowo wysyłane. W związku z tym moje pytanie jest takie: czy takie przesyłki telefoniczne mogły być generowane przez operatora Pegasusa?

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za pytanie. W ciągu ostatnich kilku dni obserwowaliśmy uważnie to zjawisko, które pan opisał, i jesteśmy bardzo zaniepokojeni tym, na co wskazują wysiłki zmierzające do zmiany kierunku śledztwa w tej sprawie oraz stworzenia problemów dla tych, którzy są wyraźnie ofiarami ataku hakerskiego. Chciałbym jednak zwrócić uwagę, że spoofing, podszywanie się pod numer telefonu w celu wysyłania wiadomości tekstowych, jest, niestety, bardzo łatwe pod względem technologicznym, a to sprawia, że tego typu działania są ulubioną aktywnością trolli i tych, którzy mogą chcieć stwarzać problemy i nie ponosić odpowiedzialności. Z pewnością byłoby możliwe robienie czegoś takiego, gdyby urządzenie zostało zhakowane za pomocą Pegasusa, ale niestety istnieje o wiele łatwiejszy sposób na to. I to według mnie pokazuje, że rozmowa dotycząca zrozumienia, co się tutaj wydarzyło, odbywa się niestety w kontekście tego, co wygląda na groźby i nękanie ofiar, a to moim zdaniem jest kolejnym sygnałem, dlaczego powinniśmy bardzo martwić się o ten przypadek i o kwestię odpowiedzialności za tę sprawę. Dziękuję za pytanie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję.
Bardzo proszę o zadanie pytania pana posła Michała Gramatykę.

POSEŁ
MICHAŁ GRAMATYKA

Bardzo dziękuję, Panie Przewodniczący. Bardzo dziękuję za możliwość zadania pytania na posiedzeniu senackiej, bądź co bądź, komisji.

Szanowni Państwo, jesteście w środowisku ekspertów firmą, która jest znana z opracowania metodologii pozwalającej na ujawnienie ataków Pegasusa na urządzenia działające pod kontrolą systemu iOS. Czy dysponują państwo podobną metodologią umożliwiającą ujawnianie ataków w innych systemach, takich jak Symbian, Android czy Windows Phone?

I dodatkowe pytanie. Czy w przypadku pana mecenasa Giertycha posiadają państwo kryminalistyczne dowody, że jego telefon był łamany Pegasusem poza granicami Polski, w momencie, kiedy przebywał poza granicami Polski i polskiego internetu? Bardzo dziękuję.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo proszę o odpowiedź.

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. W odpowiedzi na część pańskiego pytania, co do wykrywania ataków na telefonach z systemem Android, Symbian, Windows Phone lub działających na innych platformach, powiem, że dysponujemy odpowiednimi technikami, jednak mamy tu pewne ograniczenia, ponieważ zazwyczaj ilość danych rejestrowanych przez telefon z, powiedzmy, Androidem jest o wiele mniejsza niż ilość danych zapisujących się w logach

iPhone'a. Tak więc mamy wtedy mniej danych, które możemy przeszukać, a w szczególności dane te nie obejmują takiego czasu wstecz, więc jest mało prawdopodobne... Jest to możliwe, ale mało prawdopodobne, abyśmy byli w stanie zajrzeć do telefonu z systemem Android w 2022 r. i stwierdzić istnienie dowodów na to, że ten telefon został zhakowany kilka lat wcześniej, a to ze względu na inny sposób rejestrowania danych w Androidzie i fakt, że nie rejestruje on tak wielu informacji, jak to jest w przypadku iPhone'a.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, co do drugiej części pańskiego pytania, dotyczącej mecenasa Giertycha, to jeśli spojrzeć na daty zainfekowania, które zidentyfikowaliśmy i które, jak sądzę, zostały w tym przypadku upublicznione, to rozumiem, że przynajmniej w jednym z przypadków mecenas Giertych rzeczywiście przebywał w innym kraju europejskim – oczywiście zdajemy się na niego, jeśli chodzi o jego ruchy w tym czasie. Ogólnie rzecz biorąc, to także jest bardzo niepokojące odkrycie i uzasadniałoby ono dalsze dochodzenie.

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo.

Ja mam od siebie jeszcze ostatnie pytanie, dotyczące tego, czy dane zbierane przez Pegasusa w Polsce mogły zostać przekazane za granicę kraju, do firmy powiązanej z rządem obcego kraju. Państwo odpowiedzieli na to pytanie, że jest to prawdopodobne, ale że nie macie stuprocentowej pewności i stuprocentowych dowodów. Czy tak mam rozumieć państwa konkluzję, że nie wiadomo do końca, ale jest to prawdopodobne, że dane, w tym wrażliwe polskich obywateli, mogą być poza granicami kraju w wyniku operacji Pegasusem? To jest pierwsze pytanie.

Po drugie, czy prawdą jest, czy możecie państwo potwierdzić, że są 2 kraje czy 2 rządy, czy 2 agencje 2 państw, które mają innego typu technicznie umowę z firmą NSO, czyli że nie przechodzą te dane przez serwery tej firmy? Chodzi o Izrael i Stany Zjednoczone, przynajmniej Stany Zjednoczone od czasu, kiedy wykryto, że atakowano Pegasusem wielu wysokiej rangi urzędników Departamentu Stanu, czyli dyplomacji amerykańskiej. Bardzo proszę o wyjaśnienie, czy większość krajów ma inną umowę z NSO technicznie, niż te 2 kraje, czyli Izrael i Stany Zjednoczone. Dziękuję.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Panie Senatorze, dziękuję za pytanie. Po pierwsze, wyzwaniem w przypadku Pegasusa, podobnie jak i innych programów szpiegujących, jest to, że nigdy nie możemy poznać wszystkich elementów, co wynika z jednego punktu przewagi technologicznej. Mimo to sądzę, że uzasadnione jest stwierdzenie, iż byłoby niedopuszczalną lekkomyślnością, gdyby służby bezpieczeństwa nabyły i wykorzystywały Pegasusa dla ważnych priorytetów bezpieczeństwa narodowego i wywiadu bez wyraźnej oceny, jakie materiały mogą zostać ujawnione NSO Group, a w następstwie – jakiemuś innemu krajowi. Nie sądzę, by bez takiej oceny służby bezpieczeństwa były w stanie zagwarantować poufność swoich priorytetów, a tym bardziej poufność danych obywateli, którzy mogliby być objęci dochodzeniem, ale nigdy nie zostaliby postawieni w stan oskarżenia, albo których dane zostałyby skądinąd wykradzione i przeniesione przez system – a co do obu przypadków wyraźnie istnieją obawy.

Co do pytania o to, gdzie Pegasus może być używany i kto może z niego korzystać, to z publicznych oświadczeń wiemy, że teoretycznie klienci Pegasusa nie mogą namierzać amerykańskich numerów telefonów, podobnie jak zagraniczni klienci Pegasusa – a więc nie izraelscy klienci Pegasusa – nie mogą namierzać izraelskich numerów telefonów. Tak mówiły oświadczenia składane wielokrotnie przez NSO i szeroko relacjonowane. Jednak, podobnie jak w przypadku prawie każdego innego oświadczenia NSO, zachęcałbym do zdrowego sceptycyzmu.

Proszę jeszcze mojego kolegę Billa Marczaka o krótki komentarz na temat tego, jakich działających operatorów Pegasusa dostrzegliśmy na terenie Polski.

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję, Panie Senatorze, za pytanie, i dziękuję tobie, John. Jeśli chodzi o kontekst Polski, to powtórzę, że obserwowaliśmy operatora „Orzeł Biały", czyli operatora, który, z tego, co wiemy, prowadził zdecydowanie masę obserwacji w Polsce. Jest jeszcze jeden operator, którego widzieliśmy, on, jak sądzę, prowadził niewielka liczbę inwigilacji na terenie Polski. Ale to operator „Orzeł Biały" jest zdecydowanie największym operatorem, który prowadził najwięcej inwigilacji w Polsce.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Parafrazując to, co właśnie powiedział mój kolega Bill Marczak, możemy, jak myślę, powiedzieć, że tak naprawdę tylko jeden operator był mocno aktywny w Polsce i tym operatorem jest „Orzeł Biały".

PRZEWODNICZĄCY
MARCIN BOSACKI

Dziękuję bardzo panom za te wyjaśnienia. Dopytam jeszcze: ten drugi operator nie jest operatorem, który działa w Polsce, tylko z zewnątrz Polski? Zajmuje się Polską – tak? Z jakiegoś innego kraju?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. Ten drugi operator jest uważany za zagranicznego, spoza Polski, i ma on szeroki zakres międzynarodowych celów ataków, nie tylko w Polsce, ale też w wielu innych krajach na świecie.

STARSZY ANALITYK W THE CITIZEN LAB
W MUNK SCHOOL OF GLOBAL
AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
JOHN SCOTT-RAILTON

Chciałbym tylko dodać do tego, co powiedział mój kolega Bill Marczak, że oceniamy, iż priorytety i działania tego operatora są w wysokim stopniu niespójne z tymi atakami, które do tej pory były zgłaszane, a więc ze skierowanymi przeciwko tym 3 osobom w Polsce. Przedstawiliśmy to po prostu w celu uzupełnienia informacji, a nie dlatego, że wg nas istnieje poważne prawdopodobieństwo, że to ten operator jest odpowiedzialny za przypadki, o których tu dziś rozmawialiśmy.

PRZEWODNICZĄCY
MARCIN BOSACKI

Serdecznie...
(*Senator Wadim Tyszkiewicz*: Jeszcze...)
Nie, już skończmy, Panie Senatorze. Jeśli to nie jest konieczne, tobym prosił o...
(*Wypowiedź poza mikrofonem*)
Bardzo proszę. Ale ostatnie i krótkie. Już zapowiadaliśmy, że kończymy.

SENATOR
WADIM TYSZKIEWICZ

Krótkie pytanie. Czy operator, czy ktoś posługujący się Pegasusem, może przez nasz telefon wejść na konto bankowe i wpłacić pieniądze jako prowokację na przykład, żeby udowodnić i kogoś oskarżyć, lub wypłacić? Czy jest możliwość wejścia na konto bankowe, korzystając z wszystkich loginów i haseł dostępowych?

STARSZY PRACOWNIK NAUKOWY
W THE CITIZEN LAB W MUNK SCHOOL
OF GLOBAL AFFAIRS & PUBLIC POLICY
NA UNIWERSYTECIE W TORONTO
BILL MARCZAK

Dziękuję za pytanie, Panie Senatorze. Z pewnością jest to możliwe, z uwagi na to, że istnieje

możliwość pobrania hasła oraz wykorzystania aplikacji w telefonie czy manipulowania nią. Co ciekawe, udokumentowaliśmy taką sprawę w przypadku osoby z Bliskiego Wschodu, Ahmeda Mansoora, który nie tylko był namierzany za pomocą Pegasusa, ale także z jego konta bankowego zniknęła duża suma pieniędzy – myślę, że było to ok. 150 tysięcy dolarów amerykańskich. Oczywiście nie byliśmy w stanie w 100% udowodnić, że istnieje tam techniczne powiązanie, ale z pewnością istnieje możliwość, że przechwycenie czyjegoś hasła do banku online lub manipulowanie aplikacją w zainfekowanym telefonie potencjalnie zostanie wykorzystane do wypłacenia lub wpłacenia pieniędzy.

PRZEWODNICZĄCY
MARCIN BOSACKI

Bardzo serdecznie obu panom z Uniwersytetu w Toronto dziękujemy. To było dla nas bardzo ważne. To jest początek działań naszej komisji i takie ustalenie faktów co do rodzaju i skali do tej pory ujawnionych przypadków inwigilacji Pegasusem w Polsce jest dla nas absolutnie kluczowe.

Zastrzegamy sobie możliwość kontaktu z panami w przyszłości. Jeszcze raz dziękujemy za udział w posiedzeniu komisji.

Proszę państwa, jeśli pozwolicie... Uważam, że ta rozmowa, trwająca prawie 2 godziny, pozwoliła nam ustalić, według wiedzy jednych z najlepszych specjalistów od spraw cyberbezpieczeństwa na świecie, przynajmniej 3, może 4 rzeczy.

Po pierwsze, że Pegasusa w Polsce używano, używano wobec tych 3 osób, czyli pana senatora Krzysztofa Brejzy, pana mecenasa Romana Giertycha i pani prokurator Ewy Wrzosek.

Po drugie, że te inwigilacje miały, jak na skalę obserwowaną w różnych innych krajach, wymiar bardzo agresywny.

Po trzecie – i to chyba jest wiadomość z dzisiaj, pierwszy raz podana – że mogą specjaliści z Citizen Lab potwierdzić, że nie tylko operowano Pegasusem w telefonie senatora Brejzy, ale również że ściągano duże ilości danych z tego telefonu do systemu Pegasus, który, i to też jest ważne dla pracy naszej komisji, został... Jego aktywność, operatora systemu Pegasus w Polsce, czyli „Orła Białego", została pierwszy raz odnotowana przez panów specjalistów, badaczy Citizen Lab, w listopadzie 2017 r., czyli mniej więcej półtora miesiąca po sfinalizowaniu prawdopodobnego zakupu tego oprogramowania, tego systemu, tej broni cybernetycznej dla polskich służb – o tym będziemy rozmawiali jutro z oboma szefami NIK, byłym i obecnym.

Wreszcie, że obiecują panowie, że będzie więcej informacji i szczegółów, co do jakich form szpiegostwa, jeśli chodzi o te 3 telefony – pana senatora Brejzy, pana mecenasa Giertycha i pani prokurator Wrzosek... Będziemy mieli więcej informacji co do rodzaju ściąganych stamtąd danych.

Wreszcie mój ostatni wniosek jest taki, że wiarygodność tych informacji potwierdza współpraca z Citizen Lab bardzo poważnych firm elektronicznych, takich jak Apple, WhatsApp i inne, które w wyniku działań Citizen Lab poprawiały zabezpieczenia swoich produktów oferowanych dookoła globu. A również, że są rządy, jak słyszymy, jeśli chodzi o Meksyk, które po początkowym okresie zaprzeczania informacjom Citizen Lab, potem współpracują i potwierdzają ustalenia badaczy z Toronto.

Proszę państwa, na tym kończę dzisiaj posiedzenie komisji.

Zapraszam państwa na jutro, na 10.30. Naszym pierwszym gościem będzie były prezes Najwyższej Izby Kontroli, senator Krzysztof Kwiatkowski, a potem obecny prezes NIK Marian Banaś.

Dziękuję państwu bardzo. Zamykam posiedzenie komisji.

(Koniec posiedzenia o godzinie 15 minut 59)

Kancelaria Senatu
Opracowanie:
Biuro Prac Senackich, Dział Stenogramów
Druk i łamanie:
Centrum Informacyjne Senatu, Dział Wydawniczy