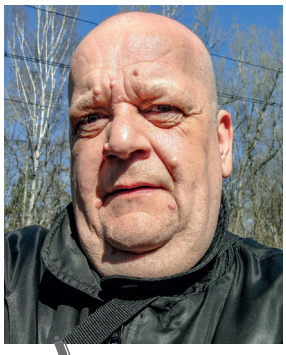
Nie dajmy się skopać Pegazowi

Nie ma przesady w stwierdzeniu, że ostatnie 30 lat rozwoju techniki to dzieje ogołacania człowieka z prywatności przez urządzenia IT. Z każdym rokiem przybywało bowiem problemów dotyczących bezpieczeństwa danych, a jednocześnie coraz więcej danych odnosiło się do naszego życia prywatnego.

Tomasz Kulisiewicz
sekretarz Sektorowej Rady ds. Kompetencji – Informatyka



Jacek Grabowski
wieloletni dziennikarz prasy komputerowej

W pamięci komputerów z czasem zaczęliśmy gromadzić prywatne zdjęcia i notatki, badania lekarskie, dowody płatności i wpływów na nasze konto oraz wiele innych dokumentów, pozwalających precyzyjnie odtworzyć wszystkie nasze czynności, prześledzić znajomości, hobby, czy te najbardziej skryte preferencje seksualne. Obecnie najwięcej takich wrażliwych danych mieści się oczywiście w smartfonie.

Specjaliści od bezpieczeństwa informatycznego mówią półżartem, że jesteśmy tyle warci, ile są warte nasze dane. Z punktu widzenia policji „tajnych, widnych i dwupłciowych" aktywność większości ludzi nie jest warta angażowania sił w zdobywanie zawartości pamięci ich smartfonów. Ale, jak wiemy, przypadki podsłuchiwania zdarzają się – i są coraz częstsze. Dlatego też hasło „Pegasus" coraz śmielej przebija się na nagłówki gazet i paski informacyjne. Niemal otoczone legendą oprogramowanie szpiegujące, opracowane przez izraelską firmę NSO Group, miało być wykorzystywane do śledzenia opozycji, ataki tego systemu na swoje telefony rzekomo odnotowali też funkcjonariusze NIK.

Miłe złego początki

Sławny Kevin Mitnick, dwukrotnie skazany w latach 90. za włamania do systemów komputerowych (na wymiar drugiego wyroku wpływ miało fałszywe oskarżenie, że używając gwizdka naśladującego wybieranie tonowe może się włamać do systemu NORAD i wywołać wojnę nuklearną), późniejszy konsultant do spraw cyberbezpieczeństwa i współwłaściciel specjalistycznych firm, w których pełni m.in. funkcję Chief Hacking Officer, włamywał się do systemów komputerowych i central poprzez linie telefonii stacjonarnej. Klonowanych komórek używał tylko dla zacierania swoich śladów włamań.

Według artykułu opublikowanego przez Kaspersky Lab w 2014 r. pierwszym wirusem na telefony komórkowe (a ściślej – robakiem, bo był samoreplikujący i nie potrzebował, jak wirusy, nośnika w postaci zainfekowanego pliku wykonywalnego) był Cabir, zwany też SymbOS/Cabir, Symbian/Cabir i EPOC.cabir, który pojawił się w 2004 r., atakując ówczesną nowość – telefony Nokii z procesorami ARM, pracujące pod kontrolą systemu SymbianOS (Nokia 7650, Nokia 3650, Nokia Communicator 9000 i kolejne). Cabir był raczej ćwiczeniem grupy prezentującej się jako A29, która chciała wskazać na zagrożenia – nie umożliwiał kradzieży danych, nie szyfrował pamięci ani nie kasował jej zawartości. Jedynymi widomymi efektami były napis Cabir pojawiający się na wyświetlaczu po włączeniu telefonu oraz rozładowanie baterii w ciągu 2–3 godzin, co wtedy było bardzo zaskakujące, bo np. niezapomniana Nokia 6310i (z systemem NokiaOS i Javą) działała nawet przez 6 godzin nieprzerwanej rozmowy i wymagała ładowania dopiero po 17 dniach czuwania. Szybkie rozładowywanie zaatakowanego telefonu powodowane było tym, że Cabir nieustannie przeszukiwał otoczenie, by móc przeskakiwać na pobliskie telefony, korzystając z transmisji Bluetooth. Jego wersja zwana Mabir potrafiła się upowszechniać także poprzez MMS-y. SymbianOs został jednak uszczelniony, a w 2012 r. Nokia z niego zrezygnowała, więc twórcy wirusów szybko przestawili się na dużo bardziej „przydatne" dla nich malware na Javę. W latach 2009–2010 pojawiły się trojany i botnety działające w środowisku Androida i iOS. Ich działanie nie ograniczało się tylko np. do wysyłania bez wiedzy użytkownika spamowych SMS-ów czy SMS-ów na płatne numery. Zaczęło się przejmowanie telefonów użytkowników w celach zdecydowanie przestępczych, a wraz z rozwojem bankowości mobilnej – przechwytywanie i przekierowywanie dostępu do kont bankowych. W 2012 r. malware znalazło się nawet w App Store i Android Market (jak wtedy nazywał się Google Play).

Antenaci Pegasusa

W 2009 r. w sieci jednego z operatorów Zjednoczonych Emiratów Arabskich rozesłany został SMS z linkiem dla klientów biznesowych smartfonów BlackBerry. Rzekoma aktualizacja bezpieczeństwa instalowała na nich oprogramowanie szpiegujące.

Już w 2012 r. specjaliści zwrócili uwagę na mobilne wersje oprogramowania RedOctober, znanego już wcześniej z atakowania desktopów, głównie agencji rządowych i służb dyplomatycznych. W tym samym roku pojawiły się też mobilne wersje programu znanego od 2011 r. FinFisher/FinSpy – dla środowisk Androida, iOS, Windows Mobile, Symbiana i BlackBerry. Oprogramowanie to potrafiło uruchamiać ukryte połączenia w celu podsłuchu otoczenia zainfekowanego telefonu, pobierać z niego logi rozmów wychodzących i przychodzących, wiadomości tekstowe i MMS-y, śledzić współrzędne GPS właściciela telefonu i wszystkie te informacje przesyłać do centrum podsłuchu. Wersje dla poszczególnych systemów miały też dodatkowe funkcje (np. FinSpy dla Symbiana potrafił wysyłać zrzuty ekranowe, dla BlackBerry – monitorować połączenia przez BlackBerry Messengera, dla Androida – włączać i wyłączać tryb samolotowy). Programy o takich właściwościach były znane wcześniej, nowością było to, że FinSpy został opracowany przez zarejestrowaną w Wielkiej Brytanii firmę Gamma Group International, która wtedy chwaliła się na swoich stronach WWW tworzeniem dla agend rządowych zdalnych narzędzi do monitoringu.

Pierwsze informacje na temat zakupu od włoskiej firmy Hacking Team i stosowania oprogramowania RCS System szpiegującego telefony komórkowe w Polsce pojawiły się w serwisie niebezpiecznik.pl już w czerwcu 2014 r., od lipca 2015 r. w serwisie jest już widoczna faktura za zakup na kwotę 178 tys. EUR i inne szczegółowe dane, pozyskane przez… włamywaczy na serwery Hacking Team. Natomiast informacje o Pegasusie pojawiły się w serwisie

w sierpniu 2016 r., a staranny opis działania systemu – w grudniu 2019 r. Czym jest więc ów izraelski Pegaz i czy możemy się przed nim zabezpieczyć?

Malware jako broń cyberwojen

Pierwszym użyciem złośliwego oprogramowania w niewypowiedzianej czy niewidzialnej wojnie było wpuszczenie wirusa Stuxnet do lokalnej sieci sterującej wirówkami w irańskim zakładzie wzbogacania uranu. Według niepotwierdzonych (przez nikogo) danych wirus zniszczył 20% działających wirówek, co mocno przyhamowało irański program stworzenia broni nuklearnej.

W różnych serwisach omawiane są liczne przypadki ataków różnych grup formalnie niezwiązanych z żadnym rządem czy armią, choć kierunki czy obiekty ataku – albo struktury państwa „nielubianego" w jakimś kraju, albo aktywiści ruchów obywatelskich niecieszący się szczególnym uznaniem władz – mogą wskazywać na jakieś powiązania. Do takich incydentów zaliczane są m.in. zmasowane ataki DDoS na estońskie instytucje publiczne, w tym parlament i rząd, banki oraz media w kwietniu 2007 r., po przeniesieniu pomnika „Brązowego Żołnierza" na cmentarz wojskowy. Polityczną reakcją obronną NATO na ten incydent było utworzenie w Tallinie w 2008 r. NATO Cooperative Cyber Defence Center of Excellence (CCDCOE). W 2008 r. seria cyberataków poprzedziła rosyjsko-gruziński konflikt o Osetię. Co najmniej od dziewięciu lat trwają cyberataki na Ukrainę – w tym w 2015 r. ataki trojanem Black-Energy na ukraiński system dyspozycji mocy, ataki (głównie na instytucje publiczne Ukrainy) szyfrującymi lub nadpisującymi sektor MBR dysków wirusami z rodziny Pietia w 2017 r. i najnowsze (od stycznia 2022 r.) ataki na centralne rządowe strony WWW Ukrainy.

Bogatą historię ma cyberwojna między Iranem a Izraelem – choć oficjalnie rządy obu krajów zaprzeczają wszelkim medialnym informacjom na ten temat. Kilka epizodów z ostatnich lat: w kwietniu 2020 r. miał miejsce atak na sterowanie infrastrukturą wodno-kanalizacyjną w różnych miejscowościach Izraela, w odwecie w maju 2020 r. zaatakowane zostały systemy logistyczne w wielkim irańskim porcie Shahid Rajaee w Bandar Abbas nad Cieśniną Ormuz. W październiku 2021 r. zaatakowano systemy 4,3 tys. irańskich stacji benzynowych, które musiały przejść na tryb ręcznego sterowania, a przywracanie sprawności trwało 12 dni.

Jak to działa?

W 2016 r. – dawno, warto to odnotować, bo oprogramowanie szpiegujące jest cały czas aktualizowane i zmieniane – pojawiła się w Sieci w formie pliku PDF instrukcja do systemu Pegasus. Większość wiedzy o nim pochodzi właśnie stamtąd lub jest pochodną opublikowanych tam informacji, co do których nie może być pewności, czy nie są dezinformacją. Według nich Pegasus to system łączący hakerskie oprogramowanie szpiegujące oraz sprzęt do rejestracji podsłuchiwanych danych i prowadzenia korespondencji z botami zbierającymi dane, które są zwykle poprzez exploity instalowane na telefonach inwigilowanych osób. Wyczerpujące informacje na temat Pegasusa dostępne są na stronie: https://niebezpiecznik.pl/post/jak-wyglada-rzadowy-trojan-pegasus-od-srodka/).

Najczulszym punktem w działaniach tego systemu jest konieczność niezauważalnego dla właściciela zdobycia kontroli nad jego telefonem. Można to osiągnąć kilkoma metodami.

Rezydent Pegasusa wkrada się do pamięci urządzenia, najczęściej wykorzystując luki *zero-day* w systemach operacyjnych lub aplikacjach. Exploit *zero-day* działa na lukach, które do momentu jego wykorzystania nie zostały jeszcze odkryte ani przez użytkowników, ani producentów oprogramowania. Wszystko dzieje się w sposób przezroczysty i nie wymaga żadnej interakcji właściciela infekowanego smartfona. Nie zawsze jest to jednak możliwe. Wtedy sięga się po metodę fałszywej flagi, czyli np. podsuwa właścicielowi telefonu jakiś adres strony internetowej, po otwarciu której nastąpi zainfekowanie telefonu oprogramowaniem Pegasusa. Można też wykorzystać podatność komunikatorów typu iMessage, What's App czy Messenger, kiedy infekcja następuje po odczytaniu przez użytkownika fałszywej, złośliwej wiadomości (również SMS). Te sposoby mają jednak tę wadę, że wymagają interakcji właściciela urządzenia. Musimy podsunąć mu link czy wysłać wiadomość skłaniającą do kliknięcia. Nie jest to banalne zadanie, trzeba więc szczegółowo je opracować, najlepiej wykorzystując informacje zdobyte wcześniej innymi metodami obserwacji. Poza tym takie sposoby pozostawiają już pewne ślady w telefonie.

Istnieje jeszcze inna metoda zainstalowania Pegasusa – wykorzystanie ataku przeprowadzonego tzw. sposobem Man-In-The-Middle poprzez fałszywy BTS, czyli urządzenie zwane IMSI Catcherem. Takie urządzenie włącza się pomiędzy nasz telefon a stację bazową (BTS) operatora, przechwytując całą komunikację naszego smartfona z prawdziwym BTS-em. W ten sposób można nie tylko podsłuchiwać i nagrywać rozmowy, lecz także podsunąć fałszywe połączenie do złośliwej strony infekującej Pegasusem. Tu oczywiście potrzebna jest cała operacja, gdyż fałszywy BTS musi znaleźć się w odpowiednim miejscu, żeby został wykryty przez telefon ofiary i umożliwił wykonanie zadania. Innymi słowy, trzeba jeździć za telefonem, który chcemy podsłuchiwać.

Jest to nieco prostsze od zorganizowania odpowiedniej prowokacji i zainstalowania agenta Pegasusa ręcznie na wybranej komórce. Manualna instalacja trwa około 5 minut i operator musi mieć dostęp do urządzenia ofiary przez cały ten czas. W grę wchodzą scenariusze rodem z książek szpiegowskich:

- zaproszenie kogoś do miejsca, gdzie telefony zostawia się w „depozycie";
- podstawienie agenta (osoby), która uwiedzie/upije/uśpi ofiarę lub będzie w pomieszczeniu z ofiarą, kiedy ta bierze prysznic;
- kontrola drogowa „ze sprawdzeniem; czy telefon nie jest kradziony". Nigdy nie oddawajcie swoich telefonów nawet najbardziej nieporadnie wyglądającemu policjantowi – na tylnym siedzeniu jego policyjnego radiowozu może siedzieć niewidoczny operator Pegasusa – ostrzega niebezpiecznik.pl.

Jak widzimy, wachlarz sposobów zainfekowania smartfona jest wystarczająco szeroki, żeby potencjalną ofiarę można było próbować osaczyć z wielu stron, więc uniknięcie szpiegowania jest bardzo trudne. Biorąc pod uwagę, że Pegasus stosowany jest głównie przez służby państwowe, które mają olbrzymie możliwości i doświadczenie operacyjne, a także zasoby finansowe pozwalające na stosowanie najbardziej wyrafinowanych i kosztownych rozwiązań, to szanse na uniknięcie inwigilacji są naprawdę nikłe. Z drugiej strony opracowanie i zastosowanie exploita typu *zero-day* nie jest takie łatwe, wymaga naprawdę wielu, często bardzo kosztownych zabiegów, a inne sposoby, mogą wymagać interakcji z użytkownikiem i zostawiają więcej śladów w smartfonie. Dlatego nie należy się z góry załamywać omnipotencją służb, tylko stosować pewne zasady „cyfrowej higieny" swojego telefonu, które mogą w pewnych przypadkach znacząco zmniejszyć niebezpieczeństwo niezauważalnego zainstalowania na nim śledzącego nasze dane oprogramowania.

Jak się bronić?

Podstawowe „zasady higieny" smartfona, niezależne od producenta telefonu i systemu operacyjnego, zestawiliśmy w krótkiej ramce. Każdy z wymienionych punktów wymaga pewnych poświęceń z naszej strony, jednak specjaliści upierają się, że jeśli poważnie traktujemy zagrożenie inwigilacją, powinniśmy równie poważnie potraktować konieczność zastosowania każdego z nich w codziennej praktyce. Oczywiście stosowanie nawet całej siódemki najprawdopodobniej nie uchroni nas przed inwigilacją, jeżeli „ktoś" bardzo potrzebuje nas wyśledzić, jednak utrudni „ktosiowi" życie, a także przyczyni się do łatwiejszego zlokalizowania i wykrycia ewentualnej infekcji.

Na smartfonach Apple dodatkowo zaleca się wyłączenie usługi iMessage, która jest bardzo podatna na ataki z zewnątrz. To również trudna decyzja, gdyż jest to usługa wygodna. W „zasadach higieny" chodzi jednak o to, żeby wyeliminować słabe punkty, przez które najczęściej dochodzi do spenetrowania zawartości smartfona. Niestety, takie wygodne, dobre usługi, zwłaszcza domyślnie włączone i właściwie niekontrolowane przez użytkownika, często stają się nośnikiem infekcji różnego typu. Podobnie jednymi z najbardziej niebezpiecznych pod tym względem są domyślne przeglądarki internetowe, dlatego zaleca się stosowanie alternatywnych wobec nich rozwiązań. Mimo że te alternatywne przeglądarki korzystają zwykle z tego samego silnika, co przeglądarka domyślna, okazują się nieraz bardziej odporne na działania hakerskie.

Szczęśliwa siódemka przeciw Pegazom z CBA

1. **Codziennie restartuj telefon.**
2. **Włącz blokadę ekranu.**
3. **Nie zapominaj o aktualizacji nie tylko systemu operacyjnego, lecz także innego oprogramowania.**
4. **Staraj się nie klikać w linki otrzymane SMS-em, bądź np. e-mailem bez uprzedniej weryfikacji.**
5. **Używaj alternatywnych przeglądarek internetowych.**
6. **Zainstaluj na smartfonie pakiet oprogramowania antymalware i antywirusowego.**
7. **Używaj zaufanych usług VPN.**

Starajmy się też nauczyć nie wchodzić bezmyślnie na strony internetowe, do których linki dostajemy SMS-em. Choćby wiadomość wyglądała bardzo wiarygodnie i idealnie trafiała w nasze oczekiwania, czy też np. lęki, to lepiej powstrzymać pokusę wejścia pod podany adres i postarać się go wcześniej zweryfikować, np. na komputerze stacjonarnym, jeśli uważamy, że otrzymany link może dotyczyć czegoś naprawdę istotnego. Podobnie uważajmy na e-maile i innego typu wiadomości z linkami. Generalnie unikajmy wchodzenia pod nieznane adresy internetowe. A przynajmniej czytajmy adresy przed kliknięciem w link, bo czasem ich składnia od razu sugeruje jakieś oszustwo i wystarczy odrobina spostrzegawczości, żeby uniknąć kłopotów.

Stosujmy pakiety antywirusowe i antymalware. Mają one swoje wady, zwłaszcza ich metody heurystyczne generu-

Skrzydlaty koń czy konsola do gier

Mityczny heros Bellerofont na skrzydlatym Pegazie chciał wjechać na Olimp, jednak Pegaz dotarł na szczyt bez jeźdźca. W nagrodę Zeus przeniósł Pegaza na nieboskłon, gdzie rezyduje do dziś. Tamten Pegaz jest dość dobrze znany, przynajmniej tym, którzy odebrali staranniejsze wykształcenie, ewentualnie pamiętają go z czołówki dawnego programu kulturalnego TVP. Natomiast nie wszyscy, którzy niedawno szukali w piwnicach konsoli do gier Pegasus, wiedzą, że nazwę tę nadano jednemu z tajwańskich klonów sławnego Famicona japońskiej firmy Nintendo. Oryginalnego Famicona w latach 1983–1995 sprzedano na świecie prawie 62 mln sztuk, a jego klonów produkowanych nie tylko na Tajwanie, lecz nawet w Brazylii i w Rosji, nikt nie zliczy. Klon Famicona pod nazwą Pegasus był niezwykle popularny w pierwszej połowie lat 90. XX w. nie tylko w Polsce (dzięki importerowi, firmie BobMark International), lecz także w ówczesnej Czechosłowacji i Jugosławii.

W latach świetności Famicona i Pegasusa nikt nie miał zamiaru używać ich jako broni, skupiano się raczej na zdobywaniu cracków do gier. Najsłynniejszą grą na platformę Famicona i jego klony, w tym Pegasusa, była „Super Mario Bros" – gra o braciach Mario i Luigim, uważana za „grę wszechczasów". Przepisywano ją i importowano na wszelkie możliwe platformy sprzętowe i systemowe; na same tylko dystrybucje Linuksa powstało kilkadziesiąt wersji, co rozszerza możliwości grania w nią nawet na superkomputerach. Oczywiście są też wersje Super Mario Bros na dwa główne środowiska smartfonowe – Androida i iOS.

ją sporo fałszywych alertów, ale stanowią jednak dodatkowy element zabezpieczający. Np. producent pakietu Bitdefender chwali się na swoich stronach internetowych, że od 2017 r. jego oprogramowanie przechwytuje exploity Pegasusa. Ile jest w tym prawdy – trudno zweryfikować. Choć pełna skuteczność wydaje się nieprawdopodobna, to mogły zdarzyć się przypadki wykrycia przez Bitdefender obecności Pegasusa na telefonach. Programy tego typu mogą również znaleźć pewne przesłanki wskazujące na penetrację naszego telefonu, np. wykryć zdalny jailbreak na iPhone'ach. Warto też wspomnieć, że istnieje opracowane pod auspicjami Amnesty International (dostępne za darmo na GitHubie https://github.com/mvt-project/mvt) narzędzie MVT (Mobile Verification Toolkit), które dokonując analizy różnych śladów w telefonie, ocenia, czy był on szpiegowany czy nie. Jest to jednak raczej narzędzie profesjonalne, którego zastosowanie wymaga doświadczenia i wiedzy kryminalistycznej.

Stosowanie wirtualnej sieci prywatnej, czyli tunelowania naszej komunikacji najlepiej połączonego z szyfrowaniem transmisji, przydaje się zwłaszcza w przypadku, kiedy korzystamy z hotelowych czy dworcowych sieci Wi-Fi. Ogólnie nie zaleca się korzystania z takich sieci, jednak przy zastosowaniu VPN zagrożenie jest znacznie mniejsze. VPN pomoże także np. w przypadku zastosowania wspomnianego w artykule IMSI Catchera, czyli fałszywego BTS. Warto tu zauważyć, że najlepsze usługi VPN są płatne, więc jeśli chcemy się dobrze zabezpieczyć, musimy liczyć się z wydaniem pewnej sumy na abonament.

Jak i przed czym bronią się rządy?

W lipcu 2021 r. brytyjski dziennik „Guardian" opublikował kilka oficjalnych odpowiedzi na pytania dziennika zadane rządom krajów, których obywatele znaleźli się na listach ofiar stosowania Pegasusa, opublikowanych przez serwisy Amnesty International, oraz inicjatywy Pegasus Project wspólnego przedsięwzięcia 17 redakcji (w tym „Guardiana") i organizacji Forbidden Stories, zajmującej się badaniem działań przeciwko dziennikarzom. Lektura tych wyjaśnień jest pouczająca:

- „Indie to silna demokracja, która jest zaangażowana w zapewnienie wszystkim swoim obywatelom prawa do prywatności jako prawa podstawowego. Realizując te zasady, Indie uchwaliły ustawę o ochronie danych osobowych z 2019 r. oraz zasady dotyczące technologii informacyjnej (wytyczne dla pośredników i kodeks etyki mediów cyfrowych) z 2021 r. w celu ochrony danych osobowych osób fizycznych i wzmocnienia pozycji użytkowników platform mediów społecznościowych. (…) Zobowiązanie do wolności słowa jako podstawowego prawa jest kamieniem węgielnym indyjskiego systemu demokratycznego (…). Jednak z ankiety wysłanej do rządu Indii wynika, że konstruowana historia jest nie tylko pozbawiona faktów, ale także oparta na z góry przyjętych wnioskach. Wygląda na to, że autorzy pytań próbują się wcielić jednocześnie w rolę śledczego, prokuratora, a także ławę przysięgłych (…). Reakcja rządu Indii na informacje na temat korzystania z Pegaza była szeroko komentowana przez media i sama w sobie jest wystarczająca, aby przeciwdziałać wszelkim złośliwym twierdzeniom o rzekomym związku między rządem Indii a Pegazem. (…) Zarzuty dotyczące rządowej inwigilacji konkretnych osób nie mają żadnych konkretnych podstaw".

- Maroko: „Władze Maroka nie rozumieją kontekstu prośby międzynarodowego konsorcjum dziennikarzy Forbidden Stories, domagającego się odpowiedzi i wyjaśnień od rządu marokańskiego dotyczących narzędzi cyfrowego nadzoru NSO Group. Przypominamy, że bezpodstawne zarzuty opublikowane przez Amnesty International i przekazane przez Forbidden Stories były już przedmiotem oficjalnej odpowiedzi władz marokańskich, które kategorycznie zaprzeczyły takim zarzutom".

- Węgry: „Nic nie wiemy o jakimkolwiek rzekomym gromadzeniu danych, o które wystąpiono we wniosku. Węgry są demokratycznym państwem prawa i jako takie zawsze działały i nadal działają zgodnie z obowiązującym prawem. Na Węgrzech organy państwowe uprawnione do stosowania tajnych instrumentów są regularnie monitorowane przez instytucje rządowe i pozarządowe. Czy te same pytania zadane zostały rządom Stanów Zjednoczonych Ameryki, Wielkiej Brytanii, Niemiec czy Francji? Jeśli tak, jak długo zajęła im odpowiedź i jak zareagowały? Czy w formułowaniu pytań wspomagała konsorcjum jakaś służba wywiadowcza?"

Kilka krajów, do których się zwrócono (Azerbejdżan, Bahrajn, Dubaj, Kazachstan, Meksyk i Zjednoczone Emiraty Arabskie), nie odpowiedziało na pytania.

Konsorcjum otrzymało też kilka pism od NSO Group ze stwierdzeniami, że raport konsorcjum oparty jest na „błędnych założeniach" i „niepotwierdzonych teoriach", a analiza danych przez dziennikarzy uczestniczących w Projekcie Pegasus opierała się na „błędnej interpretacji danych, które wyciekły z dostępnych i jawnie podstawowych informacji, takich jak usługi HLR Lookup, które nie mają wpływu na listę celów Pegasusa lub nabywców jakichkolwiek innych produktów NSO".

W Polsce w styczniu br. Jarosław Kaczyński potwierdził, że polskie służby zakupiły i używają Pegasusa. Pytany o wizytę deputowanych Parlamentu Europejskiego – pod przewodnictwem hiszpańskiego europosła Estebana Gonzaleza Ponsa – która ma na celu „zbadanie nielegalnej inwigilacji opozycji przy użyciu Pegasusa" powiedział (16 lutego br.): – *To trzeba traktować jako wyjście przed szereg jakiegoś bardzo słabego, jeśli chodzi o umiejętności polityczne, i mało znanego hiszpańskiego europarlamentarzysty. Nie przypisywałbym temu faktowi większego znaczenia. Natomiast tendencja istnieje i trzeba się przed tym bronić*.

Cyberarmie

- **Od dłuższego czasu w armiach różnych krajów powstają oficjalnie lub nieoficjalnie „cyberkompanie", „cyberpułki" albo nawet „cyberdywizje". Długa lista cyberjednostek i agencji 77 krajów – od Albanii po Wietnam – jest w Wikipedii pod adresem https://en.wikipedia.org/wiki/List_of_cyber_warfare_forces. Z polskich instytucji wymieniono na niej: Centrum Operacji Cybernetycznych, Narodowe Centrum Bezpieczeństwa Cyberprzestrzeni oraz Centrum Koordynacyjnego Systemu Reagowania na Incydenty Komputerowe SKW/MON, obecnie wszystkie pod adresem https://www.cyber.mil.pl.**

- **Militarnymi siłami informatycznymi dysponują oczywiście znane potęgi militarne i informatyczne – USA, Rosja, Chiny czy Izrael, w którym w 2020 r. w firmy sektora cyberbezpieczeństwa zainwestowano 2,9 mld USD, co stanowiło 31% inwestycji w całym tamtejszym sektorze IT. Jednostka teleinformatyczna C4I armii izraelskiej chlubi się tradycjami jednego ze swych poprzedników – utworzonej w 1937 r. służby telekomunikacyjnej Hagany, paramilitarnej organizacji z czasów brytyjskiego Mandatu Palestyny. Jednostka telekomunikacyjna już w tym samym roku zorganizowała kurs dla radiotelegrafistów, dysponowała 12 tajnymi radiostacjami, a dla uniknięcia brytyjskich podsłuchów w 1938 r. wdrożyła do służby 150 gołębi pocztowych. Po proklamowaniu w 1948 r. państwa Izrael stanowiła podstawę jednostek teleinformatycznych Sił Obronnych Izraela.**

- **Według raportu Amnesty International w 2017 r. zastępca szefa zarządu politycznego armii wietnamskiej ogłosił powstanie specjalnej jednostki informatycznej, zwanej przez aktywistów ruchów obywatelskich „Force 47", w skład której weszło ok. 10 tys. specjalistów.**

- **Neutralna od pierwszej połowy XIX w. Szwecja (ostatnią wojnę prowadziła przez trzy tygodnie w 1814 r. z... Norwegią) w 1954 r. podpisała tajne porozumienie z USA, Wielką Brytanią, Kanadą, Australią i Nową Zelandią zwane Sojuszem Pięciorga Oczu, na podstawie którego szwedzka Agencja Wojskowego Rozpoznania Radioelektronicznego (FRA) Ministerstwa Obrony, podsłuchująca kogo się tylko da, przekazuje wyniki podsłuchu wywiadom krajów porozumienia. Według szwedzkiej ustawy o totalnej obronie z grudnia 2021 r. budżety szwedzkich cyberjednostek, tworzonych w ramach projektów ITF i 2ITF i współpracujących z FRA oraz z agencjami wywiadu, mocno zwiększono już od 2021 r.; mają one osiągnąć pełną zdolność obronną (bojową?) – a więc przede wszystkim odpowiednie stany osobowe – do 2027 r.**

- **NATO poświęca coraz więcej uwagi nowym obszarom cyberobrony związanym np. z komputerami kwantowymi i biotechnologiami kognitywnymi (CBT).**