

Fachowa opresja

26 stycznia 2021

Dark Matter Group z kwaterą w Abu Dhabi jest kolejną firmą hakującą dane, aczkolwiek promującą na rynku swój przebojowy bezpieczny telefon. Powstała w latach 2014/2015, ma w pełni zależną firmę Zeline działającą w Finlandii. Deklarowane przez nią cyberbezpieczeństwo stoi cokolwiek w sprzeczności biorąc pod uwagę sposób rekrutacji specjalistów.



Doświadczony inżynier IT nie wystarczy, choć kilku Finów zostało zaangażowanych na podstawie tego kryterium. Głównie personel łowiony jest pośród pracowników Agencji Bezpieczeństwa Narodowego USA (NSA) i Israel Defence Force. Wynagrodzenie 1 mln dolarów rocznie może być pokusą, ale też rodzić zastanowienie. Pytany w studio CNBC były prezes Dark Matter Karim Sabbagh o prowadzenie rekrutacji personelu wśród pracowników NSA, lub CIA celem inwigilowania obywateli zdecydowanie zaprzeczył. Kto zachowałby się inaczej wiedząc, że taka praktyka jest przestępstwem. Jednakże dyrektor techniczny NSA William Binney stanowczo odrzucił usprawiedliwienie uznając je za kłamstwo. Jako autor projektów obliczeniowych zapewnia, że nie istnieje w nich jakikolwiek pułap ograniczeń ilości gromadzonych danych. Tryliony, kwadryliony danych mogą być bez trudu przetwarzane.

W październiku 2016 roku amerykańska agencja the Intercept, w oparciu o wyniki badań włoskich opublikowała raport. Wynikało z niego, że Dark Matter jest w stanie przejąć i zarządzać danymi dowolnego urządzenia: „Udało nam się розміścić w całym mieście sondy i za naciśnięciem jednego klawisza następuje BOOM! Zainfekowane są wszystkie urządzenia i możemy nimi sterować”. Potwierdzając w 2016 roku obecność byłych pracowników wywiadu i departamentu obrony wśród swego personelu, Dark Matter zapowiedziało zatrudnienie kolejnych

250 geniuszy. W rozmowach z już zaangażowanymi pracownikami na pytania o realizację działań na rzecz bezpieczeństwa odpowiadali, że należy brać pod uwagę realia, a nie marzenia. Z czasem okazało się, że agencje pozyskanych pracowników nieoficjalnie udzielały zgody na cały proceder. Przedstawiciel Emiratów oficjalnie wyraził dumę, że tak ambitne przedsięwzięcie powstało na terenie jego kraju. Na to dziennikarze zareagowali ostrą krytyką. Reflektując się nieco, członkowie rządzącej monarchii zaapelowali o zmianę nazwy własnej, większą dyskrecję działania, by wyciszyć nieprzychylność świata wolnego słowa.

Agent wywiadu jednego kraju opłacany i wykonujący zadania na rzecz rządu innego kraju staje się wrogiem rodzimego środowiska, w którym się wychował, wykształcił i zdobył doświadczenie. Co szczególnie ważne, to fakt, że okres pracy w służbach kraju pochodzenia łączy się z dostępem do najbardziej strzeżonych tajemnic. Ktoś taki przechodząc pod obcą banderę staje się szpiegiem sprzedającym nabyte wcześniej umiejętności wykorzystywane przeciw obywatelom ojczyzny. Dziennikarze publikujący informacje dla agencji Intercept doświadczyli próby przejęcia ich strony internetowej po ujawnieniu metod i celu pracy Dark Matter.

Jako obywatele spoza Ameryki pracownicy Dark Matter mieliby kłopot z dostępem do danych jej obywateli. Zatrudnienie cennych specjalistów amerykańskich jest hakerstwem intelektualnym. Dark Matter stał się realizatorem wdrażającym Pegasusa w 45 krajach. Operację nazwano Hide & Seek (zabawa w chowanego). Zatrudniani oficerowie amerykańscy, izraelscy, pracują w oddziałach powstających na terenie Emiratów, na Cyprze, w Singapurze, Wielkiej Brytanii.

<https://www.youtube.com/watch?v=-MsmJiip-IE>

Dziennikarz izraelski obserwujący kierunki rozwoju technologii jest przekonany, że są rządy chętnie korzystające z inwigilacji własnych obywateli w celach politycznych.

Niezależnie od tego widoczna jest wiodąca rola Izraela w cyberprzestrzeni, a kraje o dużych ambicjach będą starały się dorównać. Stawianie za cel inwigilacji środowisk dziennikarskich, przeciętnych obywateli, opozycjonistów w skali świata jest szokiem i nadużyciem zarazem. Urządzenia śledzące pozwalają kontrolerom przewidzieć kolejne kroki, plany, które przy kaprysie władzy będą torpedowane, albo modyfikowane.

Próba nawiązania kontaktu z ofiarami inwigilacji spotyka się z odmową wzięcia udziału w programie, pokazania twarzy w obawie o narażenie bezpieczeństwa rodziny. Rania Dridi pracująca dla Al Arabia odkryła włamanie do swego telefonu w 2020 roku. Citizen Lab potwierdziło sześciokrotne włamanie z wykorzystaniem Pegasusa. Początkowo sądzono, że praca dla tej stacji mogła być wystarczającym powodem przejęcia danych i kontroli. Z czasem bardziej prawdopodobnym motywem włamania były kontakty z obywatelem spoza Emiratów krytycznie wypowiadającym się w sprawach polityki. Z pewnością wśród dziennikarzy innych mediów z racji kontaktów zawodowych, wielu mogłoby nagle zorientować się o powszechności zjawiska zawłaszczania danych zgromadzonych w drodze wielu zabiegów mających wzbudzić zaufanie osób będących źródłem informacji. Szereg problemów, czy przestępstw może ujść bezkarnie, gdy informacja o nich wpadnie w niewłaściwe ręce. Czy pozostaniemy bezradni wobec złośliwych programów bezszelestnie indukowanych w nasze urządzenia będące często narzędziami pracy? Cooper Quintin zaleca unikać aktualizacji, wiadomości z nieznanego źródła z linkiem, nieznanymi plikami. Najlepiej i najprościej jest zacząć traktować telefon jako urządzenie stacjonarne. Zostawiać je w domu gdziekolwiek wychodzimy. Organizacja pozarządowa EFF (Electronic Frontier Foundation) deklaruje pomoc w organizowaniu wpływu obywateli na decyzje władzy, by nie dopuścić do rosnącej tendencji korzystania z technologii przeciwko obywatelom, redukcji ich elementarnych swobód. Walka z terroryzmem nie może stać się pretekstem dla ukrycia korupcji, wymuszeniem zgody na oszustwa wyborcze, akceptacją

niehumanitarnej egzystencji. Przykładem takiej dążności jest wyrok sądu izraelskiego z 2020 roku, który ze względu na bezpieczeństwo państwa zakazał publikacji medialnych na opisywany temat. Formalnie sprzedaż technologii inwigilującej za granicę łamie prawo izraelskie. Instytucją odpowiedzialną za licencjonowanie sprzedaży technologii rzekomo obronnej jest Ministerstwo Obrony. Skoro Pegasus stosowany jest przynajmniej w 45 krajach, ktoś jest odpowiedzialny za dopuszczenie go do obrotu. Amnesty International wystąpiła do sądu izraelskiego oskarżając NSO Group odpowiedzialnością za łamanie prawa i brak dozoru ze strony Ministra Obrony. Sąd oddalił sprawę.

Dla uniknięcia ewentualnych nieścisłości zawartych w materiale filmowym Al Jazeera zwróciła się do Dark Matter, NSO Group o komentarz. Odpowiedź jaka nadeszła była krótka i odmowna.

Opracowanie: Jola

Na podstawie: [YouTube.com](https://www.youtube.com/watch?v=Ug3333333333)

Źródło: WolneMedia.net