Inwigilacja bezśladowa

25 stycznia 2021

W połowie 2020 r. dane zawarte w telefonie dziennikarza stacji telewizji Al Jazeera zostały przejęte w wyniku włamania. Przez następne miesiące współpracując z organizacją The Citizen Lab, grupa pracowników stacji odkryła niezwykłą rzecz. Oto najbardziej zaawansowana technologia szpiegująca na świecie została wprowadzona do urządzeń dziennikarzy bez ich świadomości. Skojarzono ten fakt z wypowiedzią Netanyahu: „Jednym kliknięciem rzucacie na kolana całe narody, jeśli tylko tego zapragniecie, bo nie ma systemu, którego nie można przełamać”.

O produkcji izraelskiego Pegasusa wiadomo od dawna. Po raz pierwszy odkryto go w 2016 roku. Od tej pory rządy wielu państw zakupiły go na własny użytek. Jak system działa, kto z niego korzysta a kto jest ofiarą – rzecz trudna do ustalenia, podobnie jak samo złośliwe oprogramowanie. Pytany o jego działanie minister Avigdon Lieberman nie udzielił odpowiedzi pozostawiając słodką tajemnicę jego twórcom. Reporter Al Jazeery Tamar Ahmed drobiazgowo prześledził działanie wścibskiego systemu. Miesiącami monitorował własny telefon z pomocą ludzi z Citizen Lab działających w Kanadzie, specjalizujących się w przetwarzaniu danych. Laboratorium jako pierwsze na świecie ujawniło istnienie szpiegowskiego Pegasusa w 2016 r. Odkryto wtedy tak zwane narzędzie eksploatacji infrastruktury połączonej z telefonem u działacza Zjednoczonych Emiratów Arabskich. Infiltracja doprowadziła do aresztowania Ahmeda Mansoora, który do dnia dzisiejszego przebywa w więzieniu.

Założycielowi Citizen Lab, którym jest Bill Marczak, badanie działania systemu zajęło kilka lat nim ujawnił jego naturę. Na przykładzie sprawy A. Mansoora opisuje jak udało się

zidentyfikować źródło przychodzenia dziwnych wiadomości. Zastanawiały sms-y przychodzące z niewiadomego adresu, informujące o prawach człowieka. Przesłał je do laboratorium, gdzie na zapasowym telefonie sprawdzone zostały połączenia. Całość procesu została zarejestrowana. W momencie podłączenia telefonu do sieci natychmiast zainstalowana została aplikacja śledząca. Pytanie kto był autorem, nadawcą, kto sprzedawcą. Zastosowano procedury atrybucji (przypisania połączeń). Dostrzeżono, że powtórne kliknięcie nie powtarzało zainfekowania, ale powodowało przeniesienie połączenia z siecią przez niewinną pułapkę. Powtórne kliknięcie łączyło wprawdzie z Google, ale nie wprost. Analiza przekierowania naprowadziła na adres NSO Group należący do firmy izraelskiej sprzedającej oprogramowanie Pegasus, przeznaczone do śledzenia użytkownika za pomocą jego własnego telefonu. Autorem oprogramowania jest NSO Group działająca w miejscowości Herzlia w Izraelu. Założona w 2010 r. zatrudnia około 500 specjalistów cyber przestrzeni. Dotychczasowym największym jej osiągnięciem jest właśnie Pegasus. W ocenie Citizen Lab, Izrael jest najbardziej zaawansowanym aktorem w tej dziedzinie. Uzasadnia to szczególny kierunek szkolenia armii izraelskiej – cyber włamania. Większość zatrudnionych tam osób to personel Jednostki 8200 (Unit 8200).

Specyfiką oprogramowania jest przenikanie do najbardziej osobistych danych i przejęcie ich dzięki najczęściej wykorzystywanych aplikacji. W 2019 roku WhatsApp należące do Facebooka oskarżyło NSO o przejęcie danych 14 300 użytkowników. Wywołało to zaniepokojenie ogromnej liczby osób, zwłaszcza kiedy dla niektórych konsekwencje oznaczały śmierć. Przykładem morderstwo dziennikarza Jamala Khashoggi. Jego nieustanna obserwacja dotyczyła wszelkich aspektów: tego co mówił, pisał, gdzie i z kim bywał, aż zakończyło się okrutnym morderstwem połączonym z poćwiartowaniem. Tego narzędzia używa policja w Meksyku. Pozornie służy ono śledzeniu dziennikarzy za krytyczne wypowiedzi na temat państwa, działalności policji, ale nagle inwigilowany znika.

Jeżeli dziennikarz śledczy odkrywa podejrzane zagrożenie nadchodzące w różnej postaci przez telefon, które z czasem nasila się, warto zainstalować aplikację tropiącą. Nadejście krótkiej wiadomości z linkiem z nieznanego źródła, niemal na pewno po kliknięciu w link ułatwia włamanie do zasobów danych i przejęcie kontroli nad urządzeniem. Urządzenie przejmie od tej pory każde polecenie wysłane za pośrednictwem linku. Od tej chwili urządzenie jest trwale połączone z serwerem należącym do hakerów. Użytkownik nie widzi niebezpieczeństwa, zaś hakerzy kontrolują jego wszystkie funkcje. Smartfon dla hakera nie ma żadnych tajemnic. Narzędzia eksploatacyjne warte są miliony dolarów. Aplikacja może być wykorzystywana jedynie przez krótki czas. Docieranie do dużej ilości celów przez dłuższy czas pochłania setki milionów dolarów. Kogo stać na taki koszt i kto finansuje zakupy w NSO Group. Zdaniem firmy, głównymi klientami są służby wywiadowcze. Pracownicy firmy NSO są dobrze wyszkoleni, a kiedy odchodzą z niej mogą podejmować działalność na rzecz sektora prywatnego. Twierdząc, że Pegasus sprzedawany jest wyłącznie oficjalnym przedstawicielstwom instytucji rządowych jak służby, policja, jako prywatna instytucja nie wiadomo czy są kontrolowani.

Hasłowo ujęty mechanizm systemu jako „zero click” oznacza bezśladowe włamanie. 36 dziennikarzy tylko jednej telewizji doświadczyło inwigilacji elektronicznej. Jeśli większość materiału badanego dowodzi, że najwięcej połączeń telefonów dziennikarzy stacji Al Jazeera realizuje się z serwerem Arabii Saudyjskiej, lub Qataru to rząd tego kraju prowadzi inwigilację.

Obserwacja charakteru zakupów między wspomnianymi państwami i Izraelem wskazuje, że w ramach nazwanego „układem normalizującym” sfinalizowano transakcję cyber bezpieczeństwa. Dziennikarska próba nawiązania rozmowy z wysokim urzędnikiem izraelskim odpowiedzialnym za branżę hi-tech wprawdzie telefonicznie, ale zaowocowała potwierdzeniem koordynacji współpracy obu państw w omawianej dziedzinie. Z nieoficjalnych

informacji wynika, że Emiraty osiągnęły poziom dynamicznej współpracy w ostatnim okresie. Oznacza to rozkwit szpiegostwa na zasadach ustalanych przez Izrael. Izraelski dziennikarz Yossi Melman twierdzi, że skoro nie ma żadnej oficjalnej wzmianki o faktach, to wszystko przebiegło zgodnie z planem: „z wykorzystaniem obcych paszportów i pod stołem”, ale z czasem wyjdzie na jaw. Eksport technologii jest elementem stosunków międzynarodowych i wcale nie musi ona być wykorzystana przeciw Iranowi.

Opracowanie: Jola
Na podstawie: KomputerSwiat.pl, YouTube.com
Źródło: WolneMedia.net