Izraelska firma od oprogramowania szpiegującego Pegasus przechodzi reorganizację biznesowo – wizerunkową

Niesławna izraelska NSO Group, która była wielokrotnie przyłapana na sprzedawaniu oprogramowania szpiegującego w celu hakowania elektroniki służbom wywiadowczym kilku krajów, ogłosiła, że w ramach reorganizacji na dużą skalę firma nie tylko zmieni prezesa, ale także zawęzi krąg potencjalnych nabywców jej rozwiązań. W lipcu ubiegłego roku śledztwo z udziałem dziennikarzy z całego świata ujawniło, że NSO sprzedawało agencjom wywiadowczym na całym świecie oprogramowanie Pegasus, które było następnie wykorzystywane do szpiegowania obrońców praw człowieka, dziennikarzy, polityków i działaczy różnych wyznań. Doszło do tego, że Stany Zjednoczone nałożyły na firmę surowe sankcje.

Według rzecznika NSO firma zostanie zreorganizowana, a jej szef Shalev Hulio odejdzie. Dyrektor operacyjny NSO Yaron Shohat przejmie zarządzanie. Podczas reorganizacji wszystkie aspekty działalności firmy zostaną ponownie ocenione. Oprogramowanie szpiegujące Pegasus służy do infekowania smartfonów, wydobywania z nich danych, zdalnej aktywacji kamer i mikrofonów. Grupa NSO twierdzi, że oprogramowanie jest sprzedawane departamentom rządowym w celu zwalczania

przestępców i terrorystów, a przed sprzedażą wymagana jest zgoda władz izraelskich. Okazuje się, że oprogramowanie pomogło już uratować wiele istnień ludzkich w różnych krajach. Jednocześnie NSO podkreśla, że nie kontroluje dokładnie, w jaki sposób klienci korzystają z Pegasusa.

Po zeszłorocznej aferze okazało się, że jeszcze przed medialnym szumem i sankcjami USA wyniki finansowe NSO pozostawiały wiele do życzenia. Wcześniej w mediach pojawiły się dokumenty sądowe, zgodnie z którymi wierzyciele firmy upierali się, aby firma nadal sprzedawała oprogramowanie do krajów o „wysokim ryzyku" łamania praw człowieka w celu utrzymania rentowności, a Berkeley Research Group (BRG), będący większościowym udziałowcem „matki" spółki NSO, zażądał zaprzestania podejrzanej sprzedaży, z powodu której deweloper był prześladowany w Stanach Zjednoczonych.

Według Julio firma „reorganizuje się, aby przygotować się do następnej fazy wzrostu". Nazwał Shohat „właściwym wyborem" i stwierdził, że technologie firmy „będą nadal pomagać ratować życie na całym świecie". Shohat z kolei powiedział, że NSO zadba o to, aby jej technologie były wykorzystywane do „uzasadnionych i godnych celów".

W międzyczasie ujawniane są coraz to nowe fakty związane z użytkowaniem oprogramowania Pegasus. Pod koniec lipca Komisja Europejska poinformowała o wykryciu infekcji oprogramowaniem szpiegującym urządzeń niektórych czołowych liderów UE. Również w zeszłym miesiącu pojawiły się doniesienia, że narzędzia Pegasusa były wykorzystywane do szpiegowania aktywistów w Tajlandii podczas antyrządowych protestów.

Źródło

ArriveCan czyli narzędzie Wielkiego Brata

Aplikacja ArriveCan – jak się okazuje może zostać z nami na stałe. Rząd twierdzi, że jest to bardzo użyteczne narzędzie dla przyspieszenia procesu przekraczania granicy.

ArriveCan rzekomo sprawdza przyjeżdżających podróżnych pod kątem COVID-19 i śledzi stan szczepień. Odmowa użycia aplikacji może skutkować grzywną w wysokości do 5000 dol. na mocy ustawy o kwarantannie.

W raporcie federalnego audytora generalnego z grudnia 2021 r. stwierdzono, że aplikacja ArriveCan **poprawiła jakość informacji zbieranych przez rząd na temat podróżnych**. Jednak słaba jakość danych oznaczała, że prawie **138 000 wyników testu COVID-19 nie można było przypisać do przyjeżdżających podróżnych**, **a tylko 25 procent podróżnych, którym nakazano poddać się kwarantannie w zatwierdzonych przez rząd hotelach, zostało zweryfikowanych, że w nich rzerczywiście przebywało.**

W zeszłym miesiącu, z powodu błędu ArriveCan poinstruowała około 10 200 podróżnych, aby poddawali się kwarantannie przez 14 dni mimo, że nie musieli tego robić. Wielu krytykuje dlaczego te decyzje są zautomatyzowane i pierwszeństwo ma to co nakazuje aplikacja nie to co wynika z danych.

Ostatnie aktualizacje ArriveCan aplikacji skupiły się na rozszerzenie jej aplikacji, a nie na środkach zdrowia publicznego. Na lotniczych przejściach granicznych można teraz przy jej pomocy, wypełnić formularz zgłoszenia celnego przed

przybyciem na lotnisko Toronto Pearson, Vancouver lub Montreal.

W zeszłym tygodniu rząd poinformował, że planuje rozszerzyć tę funkcję o przyloty do Calgary, Edmonton, Winnipeg, Ottawy, Quebec City, Halifax na lotnisko Billy Bishop Toronto City.

Elektroniczne gromadzenie danych związanych jest obowiązkowe na wielu granicach międzynarodowych, a formularze internetowe są coraz częściej wykorzystywane z powodów niepandemicznych. Australia obsługuje swoje elektroniczne zezwolenia na podróż wyłącznie za pośrednictwem aplikacji online, podczas gdy od przyszłego roku będzie wymagany formularz zezwolenia online do odwiedzenia Unii Europejskiej .

Kanadyjscy urzędnicy mogą planować coś podobnego. Minister bezpieczeństwa publicznego Marco Mendicino powiedział dziennikarzom w czerwcu, że chociaż ArriveCan została stworzona dla COVID-19, *„ma możliwości technologiczne, aby naprawdę skrócić czas potrzebny na kontrolę na granicy”.*

Przed pandemią Kanada rozpoczęła już cyfryzację swoich usług granicznych za pomocą innych inicjatyw, w tym instalowania kiosków celnych na głównych lotniskach począwszy od 2017 r. i wprowadzenia w 2018 r. aplikacji eDeclaration.

Wysocy rangą przedstawiciele administracji federalnej przyznają wprost, że Ottawa wykorzystuje COVID-19 jako okazję do przyspieszenia przejścia na digitalizację obsługi kontroli przemieszczania się ludzi. Rząd federalny wykorzystuje kryzys zdrowia publicznego, aby przyzwyczaić ludzi do zmodernizowanej granicy.

Według Pierre’a St-Jacquesa, rzecznika Imigracji i Unii Celnej, **około jedna czwarta osób, które wjeżdżają do Kanady samochodem z USA, nie używa wcześniej ArriveCan.**

Kanadyjska Agencja Służb Granicznych potwierdziła, że **na granicy lądowej kanadyjsko-amerykańskiej obowiązuje**

jednorazowe zwolnienie dla podróżnych, którzy „mogli być nieświadomi" przepisów. Z pięciu milionów przepraw między 24 maja a 4 sierpnia zwolnienie to zostało użyte 308 800 razy, podała CBSA.

Jest to tylko tymczasowe rozwiązanie, powiedział St-Jacques, ponieważ funkcjonariusze, którzy już czują się przeciążeni z powodu braków kadrowych, stają się „konsultantami IT" i rozwiązują problemy techniczne podróżnych, zamiast robić to, do czego zostali przeszkoleni. *„Jeśli celem aplikacji jest zwiększenie wydajności lub bezpieczeństwa podróży transgranicznych, to obecnie nie działa"* – dodaje

Burmistrzowie miast przygranicznych, izby handlowe miast przygranicznych, a nawet sklepy wolnocłowe skarżą się, że ArriveCan, wraz z innymi ograniczeniami odstrasza amerykańskich turystów.

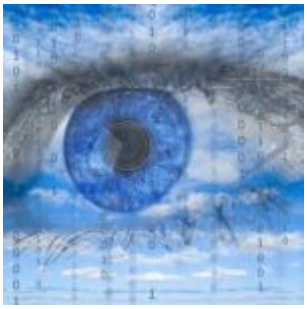
Tymczasowa przywódczyni federalnych konserwatystów Candice Bergen napisała we wtorek na Twitterze, że ArriveCan stworzył „niepotrzebne przeszkody" i „ szkodzi kanadyjskiej gospodarce i branży turystycznej".

Kandydatka na konserwatywne przywództwo Leslyn Lewis twierdzi że jest to „eksperyment nadzorowania populacji".

Komisarz ds. prywatności bada również skargę dotyczącą gromadzenia i wykorzystywania danych osobowych przez aplikację.

Źródło

Wielki Brat szpieguje cię na tysiące sposobów, a wszystkie te informacje trafiają do scentralizowanych „systemów fuzyjnych”



Wielki Brat cię obserwuje. Niestety, większość ludzi nie zdaje sobie sprawy, jak rozległa stała się siatka nadzoru. Gdy jedziesz do pracy lub szkoły, czytniki tablic rejestracyjnych systematycznie śledzą Twoją podróż. W dużych miastach tysiące wysoce zaawansowanych kamer bezpieczeństwa (wiele z nich wyposażonych jest w technologię rozpoznawania twarzy) monitoruje każdy Twój ruch. Jeśli władze wykryją, że robisz coś podejrzanego, mogą szybko przejrzeć Twoją dokumentację karną, finansową i medyczną. Oczywiście, jeśli chcą sięgnąć głębiej, telefon i komputer nieustannie tworzą skarbnicę danych z monitoringu. Nic, co robisz na którymkolwiek z nich, nigdy nie jest prywatne.

W przeszłości zebranie wszystkich tych informacji zajmowało dużo czasu. Ale teraz giganci technologiczni, tacy jak Microsoft, Motorola, Cisco i Palantir, sprzedają „systemy fuzyjne” rządom na całym świecie. Te „systemy fuzyjne” mogą natychmiast integrować dane z monitoringu z tysięcy różnych źródeł, a to całkowicie zmieniło sposób, w jaki egzekwowanie prawa jest prowadzone w wielu największych miastach.

Arthur Holland Michel jest starszym wykładowcą w Carnegie Council for Ethics in International Affairs i odbył wycieczkę po „systemie fuzyjnym” używanym przez miasto Chicago o nazwie Citigraf:

> ***Kliknął „ZBADAJ” i Citigraf zabrał się do pracy nad zgłoszonym napadem.*** *Oprogramowanie działa na czymś, co Genetec nazywa „silnikiem korelacyjnym”, czyli zestawem algorytmów, które przeszukują historyczne rejestry policyjne miasta i dane z czujników na żywo w poszukiwaniu wzorców i połączeń. Kilka sekund później na ekranie pojawiła się długa lista potencjalnych klientów, w tym wykaz osób wcześniej aresztowanych w okolicy za brutalne przestępstwa, adresy domowe mieszkających w pobliżu zwolnionych warunkowo, katalog podobnych niedawnych telefonów 911, zdjęcia i numery rejestracyjne pojazdów, które wykryto uciekające z miejsca zbrodni i nagrania wideo z wszelkich kamer, które mogły wykryć dowody samej zbrodni, w tym tych zamontowanych w przejeżdżających autobusach i pociągach. Innymi słowy, więcej niż wystarczająca ilość informacji, aby funkcjonariusz mógł odpowiedzieć na to pierwotne wezwanie pod numer 911 z niemal telepatycznym wyczuciem tego, co właśnie się wydarzyło.*

Ale te systemy służą nie tylko do tropienia przestępców.

W rzeczywistości można ich użyć do zbadania dosłownie każdego.

Przy innej okazji Arthur Holland Michel miał okazję przetestować „system fuzyjny”, który Microsoft zbudował dla Nowego Jorku:

> *Funkcjonariusz NYPD pokazał mi, w jaki sposób może wyciągnąć kartotekę każdego mieszkańca miasta, listy jego znanych współpracowników, przypadki, w których zostali nazwani ofiarą przestępstwa lub świadkami, a jeśli mieli samochód, mapę cieplną gdzie zwykle prowadzili i pełną historię ich naruszeń parkingowych. Potem wręczył mi telefon. Śmiało, powiedział; wyszukaj nazwisko.*

> *Przyszła mi do głowy fala ludzi: przyjaciele. Kochankowie. Wrogowie. W końcu wybrałem ofiarę strzelaniny, której byłem świadkiem na Brooklynie kilka lat wcześniej. Pojawił się od razu, wraz z tym, co wydawało się bardziej osobistymi informacjami niż ja, a może nawet ciekawy funkcjonariusz, miałam prawo wiedzieć bez nakazu sądowego. Czując zawroty głowy, oddałem telefon.*

Jeśli tak się dzieje w dużych miastach, takich jak Chicago i Nowy Jork, czy możesz sobie wyobrazić technologię, którą muszą teraz posiadać agencje alfabetu rządu federalnego?

Oczywiście dzieje się to nie tylko w Stanach Zjednoczonych.

Po drugiej stronie Atlantyku wspólny europejski projekt nadzoru znany jako ROXANNE budzi wiele obaw:

> *Akronim **R**eal time netw**O**rk, te**X**t, and speaker **AN**alytics for combating orga**N**ized crim**E** (Analiza sieci, tekstu i mowy w czasie rzeczywistym w celu zwalczania przestępczości zorganizowanej), został ogłoszony w listopadzie w ramach projektu opracowanego obecnie w Szwajcarii.*
>
> *Platforma biometryczna rzekomo służąca do monitorowania i rozprawiania się z przestępczością zorganizowaną, dodatkowe zastosowanie ROXANNE, które jego twórcy swobodnie reklamują, jest możliwość monitorowania osób winnych rzekomej mowy nienawiści i politycznego ekstremizmu.*

W całej Europie wprowadzane są nowe, surowe przepisy przeciwko „mowie nienawiści" i „ekstremizmowi politycznemu", a to nowe narzędzie pomoże wytropić „myślozbrodniarzy".

W szczególności to nowe narzędzie będzie intensywnie monitorować „serwisy społecznościowe, takie jak Facebook, YouTube, a także zwykłe platformy telekomunikacyjne"…

> *ROXANNE, produkt finansowany przez UE w ramach programu*

> *„Horyzont 2020", mający na celu wspieranie nowej technologii nadzoru, działa na portalach społecznościowych, takich jak Facebook, YouTube, a także na zwykłych platformach telekomunikacyjnych, aby identyfikować, kategoryzować i śledzić twarze i głosy, umożliwiając władzom stworzenie bardziej szczegółowego obrazu badanej sieci, czy to w związku z działalnością przestępczą, czy też uznaną za politycznie skrajną.*

> *Umożliwienie władzom czerpania z surowych danych z różnych źródeł i platform w celu rozpoznania typowych wzorców mowy, rysów twarzy i geolokalizacji, rezultatem końcowym jest zarówno identyfikacja podejrzanych, jak i nakreślenie skomplikowanego obrazu sieci poddawanych pod mikroskop.*

Jeśli więc mieszkasz w Europie i uważasz, że w pewnym momencie możesz być winny „myślozbrodni", możesz chcieć pozbyć się telefonu i komputera.

Poważnie.

Tam naprawdę źle się potoczyło i to tylko kwestia czasu, zanim szaleństwo w Stanach Zjednoczonych osiągnie ten sam poziom, ponieważ idziemy dokładnie tą samą drogą.

W Stanach Zjednoczonych, z każdym dniem coraz więcej głosów politycznych jest „obniżanych". Postępowy reporter Jordan Chariton początkowo wiwatował, gdy konserwatyści byli odrzucani, ale w tym momencie żałuje, że wezwał do cenzury teraz, gdy YouTube usunął jeden z jego filmów:

> *Jednak po tym, jak YouTube usunął wideo z jego własnego kanału, przedstawiające materiał z zamieszek 6 stycznia za naruszenie zasad platformy przeciwko „spamowi i nieuczciwym praktykom", Chariton zmienił swoje stanowisko.*

> *„Mając czas na refleksję i widząc atak cenzury Doliny Krzemowej, żałuję tego tweeta" – napisał progresywny*

> *dziennikarz. „Niezależnie od tego, czy niektóre kanały telewizji kablowej/YouTube wprowadzają w błąd widzów, przedstawiając nieuczciwe twierdzenia pozbawione prawdziwych dowodów, nie należy ich atakować”*

To wszystko jest zabawne, kiedy dzieje się „po drugiej stronie”, ale kiedy ci się to przytrafia, nagle staje się rzeczywistością.

Naprawdę chcą kontrolować to, co wszyscy robimy, mówimy i myślimy, a siatka nadzoru Wielkiego Brata staje się coraz bardziej dusząca z każdym mijającym rokiem.

Jeśli nie ograniczymy tej technologii, póki jeszcze możemy, to tylko kwestia czasu, zanim nasze społeczeństwo stanie się dystopijnym koszmarem o wiele straszniejszym niż cokolwiek, co George Orwell kiedykolwiek odważył się wyobrazić.

Artykuł przetłumaczono z zerohedge.com