# Indyjska aplikacja do śledzeniea COVID ujawnia lokalizację obozów wojskowych


Ekspert GIS ostrzegł, że indyjska aplikacja do śledzenia COVID, Aarogya Setu, może udostępniać lokalizacje obozów wojskowych i może być wykorzystywana przez wrogów do inwigilacji i do śledzenia ruchów żołnierzy we wrażliwych obszarach, takich jak Pangong Tso w Ladakh.

## Aarogya Setu ujawnia lokalizację obozów wojskowych

Wrażliwe informacje o rozmieszczeniu żołnierzy i ich ruchu w bazach wojskowych lub placówkach szpiegowskich wzdłuż granicy z Chinami mogły zostać naruszone przez aplikację mobilną Aarogya Setu do śledzenia COVID-19 w Indiach.

Aarogya Setu został zaprojektowany przez rząd w celu gromadzenia danych o lokalizacji i odniesienia ich do bazy danych testów COVID-19 należącej do Indian Council of Medical Research, aby ostrzec użytkownika, jeśli w pobliżu znajduje się zarażona osoba.

*„Dzięki aplikacji można sprawdzić, czy żołnierz używający Arogya Setu znajduje się w konkretnym obozie, czy też wyjeżdża do innego obozu, czy jest przenoszony, czy coś w tym rodzaju. Przez stały pomiaru, można zobaczyć, jak wiele osób zostało przeniesionych z obozu i ile osób zjnaduje się w obozie w danej chwili” Raj Bhagat Palanichamy, niezależny system informacji geograficznej (GIS)* – napisał Sputnik.

Ostrzegając władze, Raj podzielił się przykładem wykorzystania Arogya Setu do z grubsza wykrywania liczby osób korzystających z aplikacji (co może być zbieżne z liczbą żołnierzy) we wrażliwych obszarach, takich jak Pangong Tso, gdzie wojska Indii i Chin były zaangażowane w ostry konflikt od kwietnia tego roku.

*„Dzięki fałszywej aplikacji GPS możesz przenieść swoją lokalizację w dowolne miejsce. Możesz po prostu wpisać cokolwiek do Wagah Border, Pangong Tso, Galwan Valley. To nic wielkiego. A potem możesz po prostu otworzyć aplikację Arogya Setu, która pokaże, ilu zwykłych ludzi (dotkniętych COVID) jest tam itp.”-* powiedział Raj, dodając, *„że chińscy agenci mogą nie uzyskać dokładnej liczby żołnierzy w określonej lokalizacji, ale „Będą wiedzieć, czy ludzie się poruszają i czy idą w jakim kierunku, w jakim czasie itp.”*

*„Jeśli mówisz o miejscu, w którym znajduje się tylko baza wojskowa, nie jest wymagana żadna wiedza techniczna ani hakowanie. Ale jeśli chcesz dowiedzieć się czegoś o konkretnym budynku itp., trzeba trochę pokombinować ”-* powiedział Raj Bhagat Sputnikowi.

Armia indyjska, wydając poradnik w kwietniu tego roku, poprosiła żołnierzy o zainstalowanie aplikacji Arogya Setu i włączenie usług lokalizacyjnych i bluetooth podczas odwiedzania miejsc publicznych, w ośrodkach izolacyjnych, powołując się na pomoc władzom cywilnym w związku z COVID-19 podczas podczas opuszczania kwater lub stacji wojskowych. W kwietniu personel armii został ostrzeżony, aby nie ujawniał swojej tożsamości służbowej, w tym rangi, stanowiska i listy kontaktów użytkowników podczas korzystania z takich aplikacji.

## Jaki pogląd na Aarogya Setu ma Armia Indyjska?

Według wyższego rangą oficera armii, aplikacja Aarogya Setu mogłaby służyć do śledzenia lokalizacji żołnierzy, a żołnierze rozmieszczeni na wysuniętych posterunkach w ogóle nie powinni

używać telefonów komórkowych.

*„Zadbaliśmy o to, aby żołnierze rozmieszczeni na wysuniętych posterunkach nie korzystali z telefonów komórkowych. Komunikują się za pośrednictwem wojskowych urządzeń komunikacyjnych. Tak więc ich ruch ani lokalizacja nie zostaną ujawnione przeciwnikom za pośrednictwem aplikacji Aarogya Setu ”*- powiedział w poniedziałek generał armii indyjskiej Sputnikowi.

Urzędnik armii indyjskiej przyznał jednak, że ruch z posterunków pokojowych i miejsc innych niż posterunki wysunięte może być śledzony. *„Nasze oddziały patrolujące wrażliwe obszary nie używają telefonów komórkowych”* – stwierdził urzędnik.

## Przejęty kod źródłowy Aarogya Setu

12 sierpnia firma zajmująca się bezpieczeństwem cybernetycznym z siedzibą w Bombaju opublikowała szczegółowy blog wyjaśniający, w jaki sposób odkryła kod źródłowy całej platformy Aarogya Setu, w tym jej infrastruktury zaplecza udostępnionej publicznie w Internecie.

W blogu stwierdzono, że przy otwartych danych dostępowych firma była w stanie „pobrać kod źródłowy witryny internetowej Aarogya Setu, portalu Swaraksha, wewnętrznych interfejsów API, usług internetowych i wewnętrznej analizy”.

Sprawa została skierowana do Indian Computer Emergency Response Team, który po cichu załątałł lukę.

Następnie rząd zagroził Shadow Map podjęciem kroków prawnych w związku z blogiem opisującym zagrożenia bezpieczeństwa Aarogya Setu.

Chociaż dużo uwagi poświęcono Aarogya Setu, kilka rządów stanowych uruchomiło własne aplikacje COVID-19. Badanie bezpieczeństwa tych aplikacji przez Centrum Internet and

Society (CIS) okazało się, że większość z tych aplikacji nie mają konkretnej polityki prywatności.

**Żródło:**

BlacklistedNews.com