FAŁSZYWE APLIKACJE DO MONITOROWANIA COVID-19 NARZĘDZIEM W RĘKACH CYBERPRZESTĘPCÓW

Łącznie udało się zidentyfikować 12 fałszywych aplikacji do monitorowania rozprzestrzeniania się koronawirusa w społeczeństwie poprzez śledzenie kontaktów międzyludzkich. Oprogramowanie podszywające się pod oficjalne rozwiązania to nowe narzędzie cyberprzestępców, dzięki któremu rozpowszechniają złośliwe oprogramowanie - alarmują eksperci z firmy Anomali.

Według zespołu ds. badań nad zagrożeniami w cyberprzestrzeni firmy Anomali, cyberprzestępcy dystrybuują w ten sposób przede wszystkim robaki internetowe Anubis i SpyNote.

Fałszywe aplikacje do monitorowania kontaktów społecznych, które wykorzystują hakerzy, to przede wszystkim wersje na Androida. Osadzone w nich wirusy służą do wykradania danych do logowania w usługach finansowych oraz innych wartościowych danych osobowych. Według ekspertów podszywające się pod programy do walki z koronawirusem aplikacje są rozpowszechniane przede wszystkim z użyciem nieoficjalnych kanałów dystrybucji oprogramowania, takich jak strony internetowe. Żaden z programów nie był dostępny za pośrednictwem autoryzowanej platformy udostępniającej aplikacje na Androida, jaką jest Google Play.

Łącznie zespół Anomali zidentyfikował 12 fałszywych aplikacji, kierowanych do użytkowników w Armenii, Brazylii, Kolumbii, Indiach, Indonezji, Iranie, Włoszech, Kirgistanie, Rosji i Singapurze. Zdaniem ekspertów z pewnością istnieją jeszcze inne programy podszywające się pod prawdziwe aplikacje do monitorowania kontaktów - nie zostały jednakże jeszcze wykryte.

Specjaliści wskazują, że hakerzy posługujący się tego rodzaju oprogramowaniem wykorzystują zaufanie obywateli do rządowych rozwiązań technicznych do walki z epidemią koronawirusa, która - zdaniem eksperta ds. prywatności konsumenckiej w firmie Pixel Privacy Chrisa Hauka - stała się kolejną okazją do monetyzacji strachu.

Cytowany przez serwis Computer Weekly badacz radzi, aby użytkownicy szczególną wagę przykładali do tego, jakie aplikacje pobierają i instalują na swoich telefonach. Programy powinny być pobierane wyłącznie z wiarygodnych, zaufanych źródeł takich jak Google Play czy App Store (w przypadku smartfonów z systemem operacyjnym iOS).