aut. Szymon Palczewski 25.07.2019

NOWE ROSYJSKIE NARZĘDZIE SZPIEGOWSKIE. ZAAWANSOWANY PROGRAM NA SMARTFONY

Jak informują specjaliści firmy Mobile Lookout, kontrahent rosyjskiego wojska, oskarżony przez Stany Zjednoczone o wspieranie złośliwych cyberataków wymierzonych w zewnętrznych aktorów, opracował zaawansowane oprogramowanie do szpiegowania smartfonów.

Według raportu opracowanego przez ekspertów Mobile Lookout, Special Technology Center (STC) z Petersburga opracowało złośliwe oprogramowanie, którego celem jest ograniczona liczba, wyselekcjonowanych podmiotów. Wśród nich znajdują się osoby wspierające lub powiązane z rebelianckimi siłami w Syrii.

Mobile Lookout, specjalizująca się w zabezpieczaniu urządzeń mobilnych przed cyberatakami, wskazuje, że już rok temu jej specjaliści wykryli próbki szkodliwego oprogramowania wymierzonego w telefony z Androidem. Kreml stanowczo zaprzecza całej sytuacji twierdząc, że rzucane oskarżenia nie są poparte wiarygodnymi dowodami.

Eksperci Mobile Lookout nazwali złośliwe oprogramowanie „Monokle”. Może być ono obsługiwane zdalnie i komunikować się za pomocą protokołów internetowych, które były wykorzystywane do wysyłania poleceń dla innego oprogramowania stworzonego przez STC. „Monokle" to zaawansowane i w pełni funkcjonalne złośliwe oprogramowanie zawierające kilka funkcji, o których wcześniej nie wiedzieliśmy, w celu przechwytywania danych” – tłumaczą specjaliści firmy. „Monokle" może rejestrować klawisze naciskane przez użytkowników, robić zdjęcia, kręcić filmy bez zgody użytkownika, odzyskać historię przeglądarki czy aktywności w mediach społecznościowych, a także śledzić danego użytkownika. W niektórych przypadkach instalowane są fałszywe certyfikaty, pozwalające „Monokle" przechwycić zaszyfrowany ruch internetowy. Co więcej, złośliwe oprogramowanie może przechwytywać kody użytkowników do odblokowania urządzeń.

Wciąż nie wiadomo jak złośliwe oprogramowanie jest rozpowszechnianie. Badacze uważają, że może podszywać się ono pod prawdziwe aplikacje. Nie wykluczają również phisingu za pomocą smsów, emaili czy komunikatorów.

Stany Zjednoczone nałożyły sankcję na STC oraz dwie inne firmy w 2016 roku za angażowanie się w „złośliwe działania w cyberprzestrzeni”, w tym udzielanie wsparcia rosyjskiej agencji wywiadu wojskowego. STC jest głównie znana z produkcji dronów oraz innych zaawansowanych urządzeń dla rosyjskiego wojska.

Źródło: Reuters/Zdnet/CyberScoop