TWÓRCY PEGASUSA IMITOWALI FACEBOOKA, ABY INFEKOWAĆ SMARTFONY?

Eksperci Motherboard twierdzą, że odkryli nielegalną działalność NSO Group która mogła trwać przynajmniej od 2015 roku. Anonimowy informator, mający być byłym pracownikiem izraelskiej firmy twierdzi, że firma w celu infekowania smartfonów wykorzystywała witrynę sugerującą stronę należącą do Facebooka.

Redaktorzy Motherboard odkryli stronę www, która wygląda jakby należała do zespołu bezpieczeństwa Facebooka. Urządzenia końcowe użytkowników, którzy na nią weszli były zaś infekowane złośliwym oprogramowaniem. Nie stanowiłoby to większego zdziwienia, gdyby nie fakt, że eksperci twierdzą, że za witryną stoi owiana złą sławą izraelska firma NSO Group.

Informacja o działaniach miała zostać przekazana Motherboard przez byłego pracownika NSO, który miał przekazać adres IP serwera, za pomocą którego infekowano telefony Pegasusem - najpopularniejszym produktem izraelskiej firmy, który wykorzystywany jest do śledzenia użytkowników.

Oprogramowanie było przygotowane zarówno pod użytkowników z Androidem jak i iOS, a po instalacji miało możliwość śledzenia, pobierania wiadomości przesyłanych za pomocą SMS oraz komunikatorów, przekazywania danych o lokalizacji użytkownika oraz włączania kamer i mikrofonów.

Jak wskazuje anonimowy informator oprogramowanie poza stroną, która wyglądała jakby należała do zespołu bezpieczeństwa Facebooka, podszywano się również pod witrynę śledzącą przesyłki FedExu czy strony umożliwiające wypisanie się newsletterów.

Izraelska firma jest obecnie uwikłana w prawny spór z władzami Facebooka. W zeszłym roku koncern Zuckerberga pozwał izraelską firmę NSO Group, oskarżając ją o wspieranie działalności cyberszpiegów, którzy dokonali włamania na urządzenia około 1400 użytkowników. Głównym celem działań mieli być dyplomaci, politycy, dziennikarze, a także wyżsi urzędnicy państwowi z różnych stron świata. Zdaniem Facebooka NSO wykorzystywało system połączeń wideo komunikatora WhatsApp, aby w ten sposób rozsyłać złośliwe oprogramowanie na urządzenia mobilne konkretnych użytkowników. Za pomocą wirusa państwowi cyberszpiedzy mogli potajemnie śledzić właściciela telefonu, poddając jego życie nieustannej kontroli.

W trakcie batalii sądowej przedstawiciele NSO Group twierdzili, że przedstawiciele Facebooka w 2017 roku mieli zwrócić się do NSO Group z prośbą o możliwość zakupu oprogramowania szpiegowskiego Pegasus. Zgodnie z zeznaniami przedstawiciela izraelskiej firmy, Facebook chciał pozyskać możliwość monitorowania użytkowników Apple. Grupa NSO twierdzi natomiast, że odmówiła Facebookowi sprzedaży oprogramowania z uwagi na swoje wewnętrzne zasady mówiące o tym, że oprogramowanie może trafić jedynie do suwerennych rządów.