WhatsApp pozywa do sądu twórców szpiegowskiego Pegasusa

5 maja 2020

Firma WhatsApp pozwała do sądu izraelską firmę NSO Group, twórcę oprogramowania szpiegowskiego Pegasus, którą oskarża o przeprowadzenie ataku na swoje serwery i włamanie do telefonów około 1400 użytkowników WhattsAppa, w tym wysokich urzędników rządowych, dziennikarzy i działaczy praw człowieka.

Producent WhatsAppa twierdzi, że Izraelczycy ponoszą odpowiedzialność za liczne naruszenia praw człowieka, w tym włamania na telefony dysydentów z Rwandy i dziennikarzy z Indii.

Przez wiele lat NSO Group utrzymywała, że produkowane przez nią oprogramowanie szpiegowskie jest używane przez rządy w walce z terrorystami i kryminalistami. Twierdziła przy tym, że nie wie, w jaki sposób jej klienci, np. rząd Arabii Saudyjskiej, korzysta z Pegasusa.

Tym razem jednak NSO Group mogła posunąć się za daleko. W pozwie sądowym WhatsApp informuje, że prowadzone przez firmę śledztwo wykazało, że to serwery NSO Group, a nie jej klientów, brały udział w ataku na 1400 użytkowników aplikacji WhatsApp. Jak dowiadujemy się z dokumentów, ofiary najpierw odebrały połączenie telefoniczne z aplikacji i w tym momencie zostały zainfekowane szkodliwym kodem. „Następnie NSO wykorzystała sieć komputerów do monitorowania i aktualizacji Pegasusa zaimplementowanego na telefonach użytkowników. Te kontrolowane przez NSO serwery stanowiło centralny węzeł, za pomocą którego NSO kontroluje operacje prowadzone przez swoich klientów oraz sposób wykorzystania Pegasusa”.

WhatsApp twierdzi, że NSO uzyskała nieautoryzowany dostęp do

jej serwerów dokonując inżynierii wstecznej aplikacji i omijając dzięki temu zastosowane w niej zabezpieczenia, które uniemożliwiają manipulowaniem mechanizmem połączeń. Jeden z inżynierów WhatsAppa złożył zaprzysiężone zeznanie, w którym stwierdza, że w 720 przypadkach w szkodliwym kodzie, jakim zainfekowany telefony, zawarty był adres IP serwera, z którym miały się one łączyć. Serwer ten znajduje się w Los Angeles i należy do firmy, której centrum bazodanowe jest używane przez NSO.

NSO utrzymuje, że nie wie, w jaki sposób klienci tej firmy wykorzystują Pegasusa, ani kto jest celem ataków. Jednak John Scott-Railton z Citizen Lab, który pomagał WhatsApp przy tej sprawie mówi, że NSO kontroluje serwery biorące udział w ataku, zatem zna logi oraz adresy IP ofiar ataków.

Autorstwo: Mariusz Błoński
Na podstawie: FUDzilla.com
Źródło: KopalniaWiedzy.pl