Hakują Pegasusem telefony dziennikarzy Al Jazeery

21 grudnia 2020

Prywatne telefony około 36 dziennikarzy Al Jazeera zostały zhakowane przez „agentów rządowych", którzy wykorzystali kontrowersyjne narzędzie szpiegowskie niesławnej izraelskiej grupy NSO, aby podsłuchiwać, czytamy w raporcie kanadyjskiego laboratorium badawczego.

W raporcie opublikowanym w niedzielę przez Citizen Lab, jednostkę badawczą Uniwersytetu w Toronto specjalizującą się w cyberbezpieczeństwie, stwierdzono, że w lipcu i sierpniu tego roku telefony należące do pracowników katarskiej sieci medialnej, w tym dziennikarzy, producentów, prezenterów i kadry kierowniczej, zostały przejęty i zhakowane przy użyciu „niewidzialnego haku typu zero-click w IMessage".

Hak pozwolił sprawcom ataku, o który Citizen Lab „ze średnim stopniem pewności" obwiniał „agentów rządowych" z Arabii Saudyjskiej i Zjednoczonych Emiratów Arabskich, na zainfekowanie telefonów oprogramowaniem szpiegującym bez konieczności klikania przez dziennikarzy złośliwe linki.

W swoim raporcie Citizen Lab stwierdził, że tajne techniki użyte podczas ataku „były wyrafinowane", a zatem „trudne do wykrycia", ponieważ „cele" często nie zdawały sobie sprawy z czegoś podejrzanego.

Włamanie mogłoby pozostać niewykryte i tym razem, gdyby nie reporter sieci arabskojęzycznej Tamer Almisshal, który zaalarmował, że jego telefon mógł zostać szpiegowany i pozwolił badaczom monitorować urządzenie online od stycznia 2020 roku. Kilka miesięcy później, w lipcu, naukowcy zobaczyli, jak jego osobisty telefon kontaktował się z witryną internetową, gdzie został zainfekowany oprogramowaniem szpiegującym Pegasus należącym do izraelskiej grupy NSO, bez

klikania przez Almisshala.

Odkrycie skłoniło do szeroko zakrojonych poszukiwań potencjalnych innych ofiar wśród pracowników Al Jazeera, ostatecznie prowadząc zidentyfikowania łącznie 36 telefonów osobistych, które były celem udanego ataku „czterech operatorów grupy NSO". Jeden z nich, któremu grupa nadała przydomek „Monarchy", miał podsłuchiwać 18 telefonów, podczas gdy inny – nazywany „Sneaky Kestrel" – szpiegował 15 telefonów.

Grupa □□uważa, że „Monarcha" działa zgodnie z rozkazami z Rijadu, ponieważ „wydaje się , że jest skierowany głównie do osób w Arabii Saudyjskiej", podczas gdy „Podstępna Pustułka" skupiała się na dziennikarzach, którzy „ przebywali głównie w ZEA".

Badacze powiedzieli, że luka w zabezpieczeniach, która ułatwiła włamanie, została zamknięta wraz z aktualizacją IOS 14 wydaną we wrześniu, ale zauważyli, że do tego czasu prawdopodobnie była wykorzystywana na dużą skalę.

Grupa izraelska powiedziała dziennikowi „The Guardian", że „podejmie wszelkie niezbędne kroki", jeśli otrzyma „wiarygodne dowody", że jej narzędzia szpiegowskie są nadużywane.

To nie pierwszy raz, kiedy producent zestawu szpiegowskiego Pegasus znajduje się w centrum uwagi w związku z zarzutami, że jego technologia została wykorzystana przeciwko reporterom. Amnesty International poinformowała w czerwcu tego roku, że wielokrotnie nagradzany dziennikarz z Maroka Omar Radi padł ofiarą tego samego oprogramowania szpiegującego w ataku uderzająco podobnym do opisanego przez Citizen Lab.

W zeszłym roku WhatsApp potwierdził, że dziesiątki indyjskich prawników, dziennikarzy i obrońców praw człowieka znalazło się wśród 1400 użytkowników, którym włożono szpiegowskie oprogramowanie.

Pomimo kontrowersji wokół grupy NSO, izraelski sąd w lipcu stanął po stronie firmy i izraelskiego Ministerstwa Obrony w sprawie wytoczonej przez Amnesty International, która domagała się zakazu sprzedaży oprogramowania.

Opracowanie: Andrzej Kumor
Źródło: Goniec.net