Atak indyjskich hakerów na islandzką kancelarię prawną

22 maja 2025

Indyjscy hakerzy byli zamieszani w ataki na islandzką kancelarię prawną, która prowadziła m.in. grupowy pozew przeciwko Björgólfowi Thorowi Björgólfssonowi, byłemu właścicielowi Landsbankinn.

„Nie dałem im dostępu do niczego, tylko pomogłem im ściągnąć e-maile. Odpowiadałem jedynie za pomoc techniczną” – tak tłumaczył się Sumita Gupta, znany i poszukiwany haker, gdy został zapytany o działalność indyjskiej firmy BelTrox, którą prowadził przez wiele lat po ucieczce ze Stanów Zjednoczonych. Jest tam ścigany za przestępstwa komputerowe. Firma Gupty zajmowała się właśnie tym – cyberprzestępczością i włamaniami na zlecenie zamożnych klientów na całym świecie, przy pośrednictwie prywatnych detektywów z zachodnich krajów.

Wywiad z Guptą został przeprowadzony, gdy sytuacja wymknęła się już spod kontroli. Sam haker padł ofiarą wycieku danych. Sprawa była omawiana w programie „Spegillinn”.

Latem 2022 roku kanadyjska organizacja Citizen Lab we

współpracy z dziennikarzami Reuters ujawniła informacje o grupie Gupty, która od 2010 roku włamywała się do skrzynek mailowych osób prywatnych, firm, organizacji i instytucji w celu pozyskania wrażliwych danych. Jego klienci płacili ogromne sumy za te usługi. Kwoty dziesiątek milionów koron nie należały do rzadkości, zwłaszcza gdy włamania się powiodły.

Dziennikarze Reuters odkryli, że w większości przypadków ofiary ataków były zaangażowane w poważne spory sądowe, gdzie stawką były znacznie wyższe kwoty lub interesy warte ochrony. Strony w tych sprawach miały wiele do zyskania na przejęciu informacji z systemów komputerowych swoich oponentów.

Koncern naftowy ExxonMobile był jednym z dużych przedsiębiorstw, które zmuszone były reagować na doniesienia mediów i zaprzeczyć jakimkolwiek powiązaniom z BelTrox. Na celowniku indyjskiej firmy znajdowały się między innymi niezależne organizacje non-profit, które toczyły batalie z międzynarodowymi korporacjami i rządami.

W materiale Reuters przywołano wiele spraw, w których grupy, których skrzynki mailowe zostały przejęte, doświadczyły wycieku poufnych informacji do mediów lub pojawienia się ich jako dowodów w postępowaniach sądowych. Na liście celów indyjskiego BelTroxu znalazło się tysiąc prawników z 108 kancelarii. Większość z nich nie chciała się wypowiadać na ten temat, nie odpowiedziała na pytania Reutersa lub odmówiła udzielenia wywiadu. Jedną z nich była kancelaria prawna Landslög, która, podobnie jak inne, nie została wymieniona z nazwy. Nie był to jedyny islandzki cel hakera Gupty i jego ludzi. Ponadto miał on w tym kraju ważnego klienta. To, przeciwko komu skierowane były próby włamań, skłoniło dziennikarzy Reutersa do spekulacji, że w sprawę zaangażowany jest jeszcze inny islandzki podmiot, który wynajął indyjskich najemników.

„Kveik” ujawnił pół miesiąca temu, że biznesmen Björgólfur Thor w 2012 roku zwrócił się do islandzkiej firmy PPP, aby ta

szpiegowała uczestników grupowego pozwu przeciwko niemu. Pozew został wniesiony po raz pierwszy w 2011 roku, a następnie był przenoszony pomiędzy sądami różnych instancji, aż do zeszłego roku.

Björgólfur Thor zdecydował się nagle na ugodę z grupą powoda i zapłacił ponad miliard koron, aby zakończyć sprawę. Zrobił to pod pewnymi warunkami – nie przyznał się do stawianych mu zarzutów, a najwięksi indywidualni udziałowcy wśród powodów mieli nie otrzymać ani korony z tej zapłaty. Był to jego zaciekły wróg Róbert Wessman i Árni Harðarson, partner Roberta w firmie farmaceutycznej Alvogen.

Ci dwaj mężczyźni byli przedmiotem działań PPP, o których donosił „Kveik”. Ich celem było między innymi udowodnienie zaangażowanie Róberta w sprawę, a także ustalenie, skąd grupa powoda uzyskała dane, które miały posłużyć do udowodnienia rzekomych oszustw Björgólfa wobec innych akcjonariuszy upadłego Landsbankinn. PPP skierowało również swoją uwagę na Jóhannesa Bjarniego Björnssona, adwokata pracującego w sądzie najwyższym z kancelarii Landslög, który reprezentował grupę powoda w sprawie przeciwko Björgólfowi. Jego biuro było przez kilka tygodni obserwowane przez PPP, a ruch osób rejestrowany ukrytą kamerą, podobnie jak dom Jóhannesa Bjarniego. To samo dotyczyło biur firmy Alvogen oraz domów Róberta i Árniego.

W sierpniu 2020 roku cała trójka – Jóhannes Bjarni z Landslög, Róbert i Árni – otrzymała wiadomości e-mail od dziennikarza agencji Reuters. Poinformowano ich, że zgodnie z materiałami, do których dotarli reporterzy, a które wyciekły od indyjskich hakerów, oni oraz serwery Landslög i Alvogen byli celem jednego z opłaconych ataków.

Według informacji „Spegillina” kontrole bezpieczeństwa w islandzkich firmach nie wykazały skuteczności tych ataków. Dziennikarz Reuters poinformował Landslög o dokładnym czasie tych prób i przeciwko komu były skierowane. Pierwsza próba miała miejsce 20 kwietnia 2013 roku i była wymierzona w

konkretnego pracownika Landslög – Jóhannesa Bjarniego. Dane indyjskich hakerów wykazały, że w tym samym czasie podejmowali również pierwsze próby dostępu do danych przez skrzynkę mailową Árniego Harðarsona i Róberta Wessmana w Alvogen. W tym samym miesiącu Jóhannes Bjarni w imieniu grupy powoda próbował przesłuchać Björgólfa i jego ojca przed sądem.

Zestawienia pokazały również, że w latach 2016 i 2017 wielokrotnie próbowano włamać się na skrzynkę mailową Jóhannesa Bjarniego w podobny sposób. Celem była nie tylko jego skrzynka, ale także ponad 20 kont pocztowych jego współpracowników w Landslög. Okresy, w których podejmowano te próby, skłoniły dziennikarza Reutersa do zapytania pracowników kancelarii, czy ataki mogły być powiązane ze sprawami sądowymi, w których reprezentowali oni Róberta Wessmana lub Alvogen. W te same dni próbowano również zaatakować skrzynki mailowe w Alvogen. Pracownicy Landslög przeanalizowali przesłane daty i stwierdzili, że podobnie jak w 2013 roku, w tym czasie toczyły się intensywne spory związane z pozwem grupowym. Ponadto inny prawnik z tej kancelarii zajmował się dwoma innymi, niezwiązanymi sprawami przeciwko prawnikowi Björgólfa, reprezentując Róberta Wessmana.

W odpowiedzi Landslög dla dziennikarza Reutersa czytamy dosłownie: „W odniesieniu do Pana pytania, wydaje się, że istnieje zbieżność czasowa między okresami, w których toczyły się główne postępowania w tych sprawach, a datami, które Pan nam przekazał”.

Tylko w nielicznych przypadkach można było stwierdzić, kto opłacał usługi hakerów z BelTrox, nawet jeśli szczegółowe informacje wskazywały, przeciwko komu były skierowane ataki. Tak jest również w przypadku Landslög i Alvogenu. Trudno będzie udowodnić, kto stał za tym, że znani indyjscy hakerzy tak usilnie próbowali zdobyć dane z islandzkich skrzynek mailowych.

Dziennikarze z programu „Spegillinn” w zeszłym tygodniu

zwrócili się do Björgólfa Thora o komentarz w tej sprawie poprzez jego rzecznika prasowego, ale nie otrzymali odpowiedzi. Wielokrotnie próbowali się również skontaktować się z byłym dyrektorem wykonawczym Novatora, Bergim Mái Ragnarssonem, również bez skutku.

Autorstwo: Monika Szewczuk
Ilustracja: TheDigitalArtist (CC0)
Na podstawie: RÚV
Źródło: IcelandNews.is