To Kaspersky Lab odkryło największą kradzież danych z NSA

15 stycznia 2019

Z nieoficjalnych informacji dowiadujemy się, że amerykańska NSA dowiedziała się o największej w swojej historii kradzieży tajnych danych od… firmy Kaspersky. Tej samej, która znajduje się pod coraz większą presją ze strony rządu USA ze względu na podejrzenia o związki z rządem Rosji.

Harold T. Martin III, były współpracownik NSA stopniowo, przez 20 lat ukradł 50 terabajtów danych należących do NSA i innych agend rządu. To prawdopodobnie największa w historii Stanów Zjednoczonych kradzież tajnych materiałów. Wśród ukradzionych danych znajdowały się niektóre z najbardziej zaawansowanych narzędzi hakerskich, jakimi posługuje się NSA.

Martin, którego proces ma rozpocząć się w czerwcu, został aresztowany pod koniec sierpnia 2016. Przeszukano jego dom, a w lutym 2017 roku postawiono mu 20 zarzutów celowego i nieautoryzowanego uzyskania dostępu do danych związanych z obroną narodową. Każdy z zarzutów zagrożony jest karą do 10 lat więzienia.

W połowie sierpnia 2016 roku dwóch inżynierów Kaspersky'ego otrzymało na Twitterze pięc tajemniczych wiadomości. Wszystkie zostały wysłane z konta HAL999999999 i wszystkie były zaszyfrowane. Gdy tylko inżynier odpowiedział na którąś z nich, komunikacja była przerywana, a jego konto blokowane, by nie mógł ponownie komunikować się z HAL999999999.

W pierwszej z wiadomości jej nadawca domagał się kontaktu z „Jewgienijem". Prawdopodobnie chodziło o Eugene'a Kaspersky'ego, dyrektora Kaspersky Lab. W drugiej, wysłanej zaraz później wiadomości, czytamy „Shelf life, three weeks",

co wskazuje, że mamy do czynienia z jakąś ofertą o ograniczonym czasie ważności.

Pół godziny później anonimowa grupa o nazwie Shadow Brokers zaczęła wypuszczać do sieci tajne narzędzia hakerskie NSA, ogłosiła, że ma ich więcej i że jest gotowa je sprzedać z milion Bitcoinów. Shadow Brokers, którzy są prawdopodobnie powiązani z rosyjskim wywiadem, poinformowali, że narzędzia ukradli wydziału hakerskiego NSA zwanego Equation Group. Wydział ten jest autorem najbardziej zaawansowanej operacji hakerskiej w historii.

Anonimowe źródła poinformowały dziennikarzy, że inżynierowie Kaspersky'ego zainteresowali się zbiegiem okoliczności pomiędzy tajemniczymi wiadomościami, a działaniem Shadow Brokers. Zaczęli zastanawiać się, czy jest to ze sobą powiązane. Powiązali konto HAL999999999 z Martinem, a jego z pracą dla amerykańskich służb. Skontaktowali się z NSA i zasugerowali, by przyjrzeć się Martinowi.

Rzecznik prasowy firmy Kaspersky odmówił potwierdzenia, czy przedsiębiorstwo było w jakikolwiek sposób zaangażowane w sprawę Martina. Nie dowiemy się też tego z dokumentów sądowych. Ich całość nie została jeszcze ujawniona, a w tych, które zostały dotychczas udostępnione, wymazano nazwiska odbiorców wiadomości z Twittera. Dokumenty te ujawniono w związku z tym, że adwokaci Martina próbowali podważyć uzyskany przez FBI nakaz przeszukania domu Martina twierdząc, iż FBI występując o nakaz nie uprawdopodobniło swoich podejrzeń. Sędzia się z tym nie zgodził, uznając, że wystarczającym podejrzeniem był zbieg czasowy wysłanych informacji z ujawnianiem tajnych narzędzi NSA przez Shadow Brokers w sytuacji, gdy Marin, jako współpracownik NSA, mógł uzyskać dostęp do narzędzi Equation Group.

Jak twierdzą anonimowe źródła, Kaspersky Lab przekazało NSA wszystkie informacje, jakie otrzymało na Twitterze wraz z dowodami, wskazującymi na ich prawdziwego nadawcę. Z

dokumentów sądowych wynika, że to właśnie stało się dowodem, na podstawie którego FBI uzyskało nakaz przeszukania domu Martina. Dokumenty sądowe nie wyjaśniają jednak, w jaki sposób FBI weszło w posiadanie informacji z Twittera, ani jak ustaliło tożsamość Martina.

Wiadomo, że w przeszukaniu jego domu brało udział ponad 20 agentów FBI oraz jednostka antyterrorystyczna, co wskazuje, na dużą wagę sprawy oraz obawy o to, z kim Martin mógł się jeszcze kontaktować. W domu podejrzanego znaleziono olbrzymią ilość tajnych materiałów, zarówno w formie papierowej jak i cyfrowej, ukradzionych w latach 1996–2016. BYły wśród nich te same narzędzia, które ujawnili Shadow Brokers. Wiadomo, że wśród nich są niezwykle zaawansowane programy wykorzystywane do śledzenia ruchów terrorystów oraz zbierania danych.

Powstaje pytanie, czy Martin dostarczył te narzędzia Shadow Brokers. Obecnie nie jest on oskarżony o szpiegostwo, a śledczy nic nie mówią, o jego kontaktach z tą grupą. Shadow Brokers zaprzeczyli, by był on jednym z nich.

Adwokaci Martina twierdzą, że brak dowodów, by chciał on komukolwiek przekazać tajne informacje, jest on patriotą, a poufne dane beztrosko zabierał do domu i tam przechowywał, gdyż cierpi na zaburzenie kompulsywne.

Kaspersky Lab znajduje się w paradoksalnej sytuacji. Martin wybrał tę firmę, gdyż z pewnością lepiej niż ktokolwiek spoza społeczności wywiadowczej wie o podejrzeniach, jakie są wobec niej wysuwane. Wielu specjalistów ds. bezpieczeństwa ufa Kaspersky Lab i nie wierzy w zarzuty, by wspomagała ona rosyjski wywiad. Jednocześnie jednak nie dziwią się władzom USA, że podejrzliwie traktują rosyjską firmę założoną przez byłego oficera wywiadu. Kaspersky, ostrzegając NSA o roli Martina, najprawdopodobnie wykonała gest dobrej woli w stosunku do USA. Gest, który może nie przynieść jej żadnych korzyści.

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