Cyberprzestępcy szantażują kancelarię prawną

14 maja 2020

Cyberprzestępcy zaatakowali i okradli kancelarię prawną obsługującą m.in. Lady Gagę, Drake'a czy Madonnę. Teraz szantażują ofiarę ujawnieniem 756 gigabajtów ukradzionych danych. Mają wśród nich znajdować się kontrakty, korespondencja prywatna czy umowy poufności.

Nowojorska kancelaria Grubman Shire Meiselas & Sacks oferuje swoje usługi przemysłowi rozrywkowemu i mediom. Jak poinformowali badacze z firmy Emsisoft, kancelaria została zaatakowana za pomocą ransomware REvil (Sodinokibi). Przestępcy ukradli m.in. numery telefonów klientów kancelarii, adresy e-mail, ich prywatną korespondencję, umowy podpisane z agencjami reklamowymi i inne dokumenty związane z pracą słynnych osób.

„Niewielką część tych danych umieszczono w internecie. Są tam zrzuty ekranowe kilku umów czy dane folderów, do których cyberprzestępcy uzyskali dostęp. Grupa twierdzi, że ukradła 756 gigabajtów danych, które opublikuje, jeśli kancelaria im nie zapłaci" – mówi Brett Callow, analityk z Emsisoft.

Grubman Shire Meiselas & Sacks obsługuje najsławniejszych ze sławnych. Jej klientami są Elton John i Rod Stewart, Lil Nas X i U2 czy tacy giganci jak Facebook, Sony oraz HBO.

„Możemy potwierdzić, że padliśmy ofiarą cyberataku. Poinformowaliśmy naszych klientów i pracowników. Zatrudniliśmy światowej klasy ekspertów, którzy specjalizują się w takich sprawach i pracujemy nad rozwiązaniem problemu" – oświadczyli przedstawiciele firmy.

Nie wiadomo, jakiej kwoty domagają się szantażyści. Jednak na poparcie swoich gróźb opublikowali dokumenty, wśród których

jest prawdopodobnie kontrakt podpisany w 2019 roku przez agenta Madonny w związku z organizacją jej trasy World Tour 2019-2020 czy inny dokument podpisany przez Christinę Aguilerę. „Ujawnienie ukradzionych informacji może prowadzić do kradzieży tożsamości, podszywania się pod kogoś, ataków phishingowych i innych rodzajów oszustw. Niewykluczone też, że przestępcy mogą próbować kontaktować się bezpośrednio z ludźmi, których dane ukradli i żądać od nich pieniędzy" – mówi Callow.

Ataki z użyciem REvil nie są niczym nowym. W bieżącym roku zaatakowano w ten sposób kilkanaście celów. Przestępcy m.in. ukradli i ujawnili dane z National Eating Disorders Association, organizacji zajmującej się pomocom osobom z zaburzeniami odżywiania. Okradli też giełdę wymiany walut Travelex i wymusili na niej zapłatę ponad 2 milionów dolarów okupu.

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