

## Cyberterrorysty zaatakowali witrynę SAS

20.02.2023

Powiązana z rosyjskim rządem grupa hakerska nazywająca siebie „Anonimowym Sudanem” przyznała się do cyberataku, który wyłączył witrynę Scandinavian Airlines (SAS) na początku tego tygodnia i zagroził bezpieczeństwu danych tysięcy klientów tej skandynawskiej linii lotniczej.

### Groźny wyciek danych

W oświadczeniu opublikowanym na swojej korporacyjnej stronie internetowej linia lotnicza wyjaśniła, że ona i „kilka innych firm” padło ofiarą cyberataku, który spowodował kilkugodzinne wyłączenie ich stron internetowych i aplikacji na smartfony.

Podczas tego cyberincydentu niektórzy podróżni, logując się na swoich kontach SAS, odkryli, że mają dostęp do danych osobowych innych klientów linii lotniczej, w tym ich imion i nazwisk, dat urodzenia, adresów pocztowych i adresów e-mail. Dodatkowo mieli dostęp do czterech ostatnich cyfr numerów kart kredytowych innych klientów tej linii lotniczej.

Pierwszą reakcją SAS było ostrzeżenie klientów przed korzystaniem z aplikacji, dopóki problem nie zostanie rozwiązany – co nie uspokoiło podróżnych, którzy obawiali się, że ich dane osobowe mogły wpaść w ręce zupełnie obcych osób. Kolejnym nieroztropnym krokiem korporacji było zdeprecjonowanie wagi tego cyberincydentu i stwierdzenie, że „takie ataki często pojawiają się partiami, a więcej ataków prawdopodobnie nastąpi w najbliższej przyszłości. Jednak” – jak powiedziała firma – „nie powinno to mieć wpływu na dane pasażerów”.

## **Kulisy cyberataku na SAS**

Atak nastąpił w ramach fali podobnych ataków pod szyldem grupy „Anonimowy Sudan” na szwedzkie organizacje. Inne przykłady incydentów przeprowadzonych w ramach tej kampanii to próba złamania szwedzkiego sektora opieki zdrowotnej za pomocą zmasowanego ataku DDoS oraz walentynkowy cyberatak, który zakończył się wyłączeniem anteny szwedzkiego nadawcy telewizyjnego SVT.

Zgodnie z informacjami udostępnianymi na kanale Anonymous Sudan Telegram cyberterrorysty twierdzą, że ich ataki są odwetem za antyislamskie demonstracje w Szwecji.

Chociaż grupa hakerska zdecydowała się używać nazwy „Anonimowy Sudan”, niektórzy komentatorzy zwracają uwagę, że sprawcy ataków z dużym prawdopodobieństwem w rzeczywistości nie pochodzą z Sudanu, tylko są w jakimś stopniu zależni od rosyjskiej Dumy. Kampania może być więc próbą destabilizacji i odpowiedzią na plany Szwecji dotyczące wejścia w szeregi NATO.

„Zespół Bitdefender zaobserwował w ostatnich latach znaczący wzrost cyberataków, które są przeprowadzane przez doskonale zorganizowane grupy hakerskie finansowane przez rządy niektórych państw. Z usług takich cyberprzestępców chętnie korzystają nie tylko kraje autorytarne, takie jak Chiny, Korea Północna, Iran i Rosja. W zasadzie czynią to wszystkie państwa i ugrupowania, które są w jakimś stopniu uwikłane w konflikty zbrojne i kryzysy dyplomatyczne. Celami ataków najczęściej padają infrastruktura krytyczna, instytuty rządowe, placówki medyczne oraz firmy związane z mediami. Obecnie nastały bardzo trudne czasy dla wszystkich administratorów sieci, dlatego zawsze apelujemy o to, aby nie zaniedbywać tematu cyberbezpieczeństwa i rozważyć integrację dodatkowych warstw ochrony, takich jak XDR i MDR” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora Bitdefender.

Źródło: <https://bitdefender.pl/cyberterrorysty-zaatakowali-witryne-sas/>  
Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 20.02.2023

Z pozdrowieniami Piotr Rozmiarek

E-mail: [piotr.r@marken.com.pl](mailto:piotr.r@marken.com.pl) | Tel. bezpośredni: 570 400 019

Informacje o firmie Bitdefender

Bitdefender to rumuński dostawca rozwiązań z zakresu cyberbezpieczeństwa oraz światowy lider chroniący miliony użytkowników. Bitdefender jest częstym zdobywcą wielu branżowych nagród i uznaną światową marką. Od 2001 roku konsekwentnie dostarcza najwyższej jakości produkty służące do zapewnienia bezpieczeństwa

zarówno użytkownikom domowym, jak i wielkim korporacjom i rządowym instytucjom. Bitdefender jest znany ze swojej innowacyjności oraz wyposażania swojego oprogramowania w najnowsze technologie, takie jak uczenie maszynowe, heurystyka oraz EDR i XDR.