BRITISH AIRWAYS ZAATAKOWANE PRZEZ MAGECART

Firma RiskIQ opublikowała szczegółową analizę ataku hakerskiego na linie lotnicze British Airways łącząc incydent z działalnością grupy hakerskiej Magecart, aktywnej od 2015 roku. Cyberprzestępcy ci znani są przede wszystkim z ataków na systemy płatności.

Grupa Magecart specjalizuje się w gromadzeniu danych finansowych pozyskiwanych z niedostatecznie zabezpieczonych systemów płatności w internecie. Eksperci z RiskIQ stwierdzili, że w przypadku ataku na British Airways cyberprzestępcy działali inaczej niż zwykle. Narzędzia, których użyli, zostały dostosowane do specyfiki infrastruktury linii lotniczych i nie były oparte o wcześniej wykorzystywany przez Magecart kod, dzięki któremu grupa była łatwo rozpoznawalna.

Jak powiedział w rozmowie z magazynem "Wired" analityk zagrożeń w RiskIQ Yonathan Klijnsma "od dłuższego czasu śledziliśmy uważnie działalność grupy Magecart. Dokonali przełomu mniej więcej w 2017 roku, kiedy hakerzy zaczęli szukać nowych celów i dostosowywać metody włamań do ich specyfiki. Chodzi tu o firmy takie, jak na przykład Ticketmaster". Jego zdaniem "atak na British Airways to kolejny element kampanii, w ramach której cyberprzestępcy przygotowali specjalne narzędzia naśladujące infrastrukturę, z jakich korzystała organizacja będąca ich celem".

Początkowo przedstawiciele linii lotniczych British Airways twierdzili, że wyciek danych nie objął numerów paszportów bądź innych wrażliwych danych osobowych pasażerów. W późniejszym czasie jednak firma wyjaśniła, że w wyniku włamania do systemów wyciekły jednak bardzo wrażliwe dane finansowe, takie jak daty ważności kart płatniczych oraz kody CVV do uwierzytelniania transakcji z ich użyciem. Przewoźnik wcześniej deklarował, że nie przechowuje kodów CVV po uwierzytelnieniu płatności.

Według magazynu "Wired", wszystkie te informacje posłużyły jako wskazówki przy identyfikacji możliwych sprawców włamania. Firma RiskIQ ocenia, że hakerzy użyli techniki krzyżowego skryptowania, polegającej na znalezieniu słabo zabezpieczonego fragmentu kodu na stronie internetowej ofiary i wstrzyknięciu w niego własnego, który zmienia działanie strony. Atak z użyciem tej techniki nie wymaga dostępu do sieci czy serwerów danej organizacji, co może, zdaniem ekspertów, tłumaczyć, dlaczego hakerzy zyskali dostęp do informacji przetwarzanych jedynie w wybranym okresie, w tym do danych, których linie BA nie przechowują w swoich bazach.

Podejrzany skrypt, który najpewniej posłużył hakerom do przeprowadzenia ataku, badacze z RiskIQ znaleźli na stronie internetowej przeznaczonej do nadawania bagażu. Ostatni raz była modyfikowana w grudniu 2012 roku - cyberprzestępcy wstrzyknęli w nią jednak 22 linijki kodu, który posłużył im do dalszych działań - zbierania informacji, jakie klienci BA wpisywali w formularze na stronie. Grupa Magecart zapłaciła nawet za własny certyfikat SSL dla serwera, na który były wysyłane dane, a wszystko aby pasażerowie nie nabrali podejrzeń - podkreślają eksperci.

Linie British Airways po wykryciu ataku poinformowały, że działaniem hakerów została dotknięta również aplikacja mobilna przewoźnika. Analitycy RiskIQ wykazali natomiast, że część aplikacji mobilnej dla urządzeń z systemem Android została zbudowana w oparciu o ten sam słabo zabezpieczony kod, jakiego użyto na stronie linii. Skrypt, który hakerzy wstrzyknęli na stronę internetową podczas ataku, wywarł wpływ również na aplikację mobilną. Zdaniem ekspertów, cyberprzestępcy wiedzieli, jak zbudowana jest aplikacja i strona British Airways i wykorzystali słabości ich konstrukcji - dlatego właśnie atak na linie lotnicze był tak skuteczny, choć mało zaawansowany technologicznie.

We wtorkowym wydaniu dziennika "Financial Times" spekuluje się o nałożeniu na British Airways dużej kary finansowej przez brytyjski odpowiednik Urzędu Ochrony Danych Osobowych - Information Commissioner's Office (ICO). Zdaniem gazety, przemawiają za tym: duża skala incydentu oraz fakt, że wyciek danych objął również kody uwierzytelniające kart płatniczych CVV.

W opinii prawników, wyciek tych kodów daje klientom British Airways podstawę do ubiegania się o odszkodowanie finansowe w związku z cyberatakiem, a kara nałożona przez ICO zgodnie z przepisami RODO obowiązującego w całej Unii Europejskiej może wynieść nawet 4 proc. globalnych dochodów firmy za ostatni rok - co w przypadku British Airways przekłada się na kwotę około 500 mln funtów.

AK/PAP