

Atak ransomware na Coca-Colę – firma zapłaciła 1,5 mln dolarów

12.09.2023

Coca-Cola FEMSA, największa na świecie franczyzowa rozlewnia Coca-Coli, rzekomo padła ofiarą ataku ransomware, w wyniku którego kierownictwo firmy zapłaciło hakerom okup za zapobieżenie wyciekowi „niektórych” plików. Ugrupowanie hakerskie znane jako „TheSnake” rzekomo zdobyło „pełną bazę danych Coca-Cola FEMSA zawierającą informacje o firmie, poufne zdjęcia i pliki oraz wiele innych” – podaje DataBreaches.net, która opisuje codzienne przypadki naruszeń i wycieków danych.

Atak ransomware na Coca-Colę

Podczas tego ataku wykorzystano oprogramowanie typu ransomware. Napastnik i jego grupa rzekomo dwukrotnie penetrowali infrastrukturę informatyczną firmy w ciągu nieco ponad roku, w wyniku czego skradł ponad 8 GB danych.

Według zrzutu ekranu opublikowanego na popularnym forum hakerskim cyberprzestępcy grozili Coca-Cola FEMSA następującą wiadomością:

„Jak powiedzieliśmy, po upływie określonego czasu Twoje dane będą stopniowo przesyłane do domeny publicznej dla wszystkich. Nadal możesz chronić swoją reputację i zachować większość danych w tajemnicy, ale masz na to coraz mniej czasu. Wybór należy do Ciebie Coca-Cola FEMSA.”

Napastnicy rzekomo uzyskali pełne informacje o firmie z Meksyku, Argentyny, Brazylii i Kostaryki, w tym: „hasła, dokumenty finansowe, faktury w formacie ZIP oraz dane dostawców, dane z obiektów, wyposażenie firmy, kampanię reklamową, dane i zdjęcia pracowników, kopie zapasowe i wiele więcej.”

Coca Cola płaci tylko za część danych

Choć pierwotnie napastnicy żądali 12 milionów dolarów za usunięcie wszystkich wyekstrahowanych plików, firma wynegocjowała zapłacenie 1,5 miliona dolarów za zapobiegnięcie wyciekowi „niektórych” plików.

„W zapytaniu wyjaśnił, że zażądali 12 milionów dolarów za usunięcie wszystkich wyekstrahowanych plików, ale firmie najbardziej zależało na zapobieżeniu wyciekowi niektórych plików, a negocjacje skupiały się na cenie za brak wycieku tych konkretnych plików”. Raporty dotyczące naruszeń danych. „Według TheSnake firma rzeczywiście zapłaciła im 1,5 miliona dolarów za zapobiegnięcie wyciekowi tych plików”.

Atak ransomware na Coca-Colę – firma zapłaciła 1,5 mln dolarów **Bitdefender**

Pozostałe pliki są nadal wystawione na sprzedaż na forach hakerskich, za które cyberprzestępcy żądają 65 000 dolarów.

„Ataki ransomware są nadal bardzo często wykorzystywane przez hakerów. Jeśli firma nie ulegnie żądaniom cyberprzestępców, to jej skradzione dane zazwyczaj są wystawiane na sprzedaż w ciemnej sieci, gdzie wszyscy mogą je pozyskać. Taka sytuacja jest nie tylko dotkliwym ciosem dla reputacji pokrzywdzonej firmy, lecz także stwarza zagrożenie dla wszystkich użytkowników sieci, których dane wyciekły, ponieważ to właśnie oni często stają się celami kolejnych cyberataków” – mówi Mariusz Politowicz z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Przypadkowo niesławna ekipa oprogramowania ransomware BlackCat (AlphV) przyznała się do ataku na Coca-Cola FEMSA i w czerwcu ujawniła podobne dane.

Po zapytaniu TheSnake zaprzeczył jakiegokolwiek powiązaniu z atakiem przeprowadzonym przez BlackCat.

Źródło:<https://bitdefender.pl/atak-ransomware-na-coca-cola-firma-zaplacila-15-mln-dolarow/>

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.

Data udostępnienia: 12.09.2023

Z pozdrowieniami Piotr Rozmiarek

Atak ransomware na Coca-Colę – firma zapłaciła 1,5 mln dolarów 

E-mail: 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.