Bitdefender

Uniwersytet East Central ofiarą ataku ransomware BlackSuit

12.04.2024

Uniwersytet East Central (ECU) w Ada w stanie Oklahoma ujawnił, że gang zajmujący się oprogramowaniem ransomware przeprowadził atak na jego systemy, w wyniku którego niektóre komputery i serwery zostały zaszyfrowane, a także mogły zostać skradzione poufne informacje. W poradniku zamieszczonym na swojej stronie internetowej ECU twierdzi, że gangowi oprogramowania ransomware BlackSuit nie udało się zablokować kluczowych usług uniwersytetu, ale „był w stanie przeprowadzić skuteczny atak na różne komputery w kampusie".

Groźny atak ransomware na amerykańską uczelnię

ECU twierdzi, że w odpowiedzi na atak zwróciła się o pomoc do zewnętrznych ekspertów ds. cyberbezpieczeństwa, zresetowała hasła studentów i ponownie oceniła swoje systemy bezpieczeństwa.

Chociaż ECU nie potwierdziło dokładnego charakteru włamania się oprogramowania ransomware do systemów uniwersytetu, jego pracownicy stwierdzili, że zaobserwowało „wzrost liczby spamu/złośliwych wiadomości e-mail w dniach poprzedzających ataki".

Pełne skutki ataku z 16 lutego są nadal badane, ale ECU ustaliło, że gang hakerski mógł uzyskać dostęp do nazwisk i numerów ubezpieczenia społecznego niektórych studentów.

Eksfiltracja wrażliwych danych osobowych grozi nową falą phishingu

Nie jest to pierwszy raz, gdy oprogramowanie ransomware BlackSuit atakuje sektor edukacyjny. Na przykład pod koniec ubiegłego roku przyznała się do serii ataków na szkoły w środkowej Gruzji, a także na uczelnię sztuk wyzwolonych DePauw University w stanie Indiana.

Gang zajmujący się oprogramowaniem ransomware BlackSuit przyznał się ostatnio do cyberataku na kalifornijską firmę Select Education Group, w wyniku której naraził poufne dane osobowe około 70 000 osób.

Pamiętajmy, że nie tylko organizacje edukacyjne muszą mieć się na baczności przed gangiem oprogramowania ransomware BlackSuit. Pod koniec zeszłego roku raport Departamentu Zdrowia i Opieki Społecznej Stanów Zjednoczonych (HHS) wydał ostrzeżenie dla sektora publicznego opieki zdrowotnej, że BlackSuit jest „podmiotem stwarzającym zagrożenie, które należy uważnie obserwować w najbliższej przyszłości".

ECU twierdzi, że „będzie na bieżąco informować swoją społeczność" o

wszelkich dodatkowych informacjach uzyskanych na temat ataku. Radzi osobom, które uważają, że może to mieć wpływ, aby odwiedziły stronę Identitytheft.gov w celu uzyskania porady, jak stwierdzić, czy padły ofiarą kradzieży tożsamości i co zrobić, jeśli ich dane zostaną zgubione lub skradzione.

„Jeśli podejrzewasz, że Twoje dane mogły zostać skradzione, lub wyciekły do sieci, to przygotuj się na to, że zostaniesz celem kampanii phishingowych. Zmień hasła, aby zapobiec potencjalnej próbie kradzieży kont i zadbaj o to, aby wszystkie Twoje hasła były unikatowe. Następnie zabezpiecz się za pomocą skutecznego antywirusa, który został wyposażony w moduł antyphishingowy. Unikaj pobierania podejrzanych załączników, klikania w niebezpieczne linki oraz uważaj na niechciane połączenia telefoniczne" – mówi Arkadiusz Kraszewski z firmy Marken Systemy Antywirusowe, polskiego dystrybutora oprogramowania Bitdefender.

Źródło:https://bitdefender.pl/uniwersytet-east-central-ofiara-ataku-ransomware-blacksuit/

Informację można wykorzystać dowolnie z zastrzeżeniem podania firmy Marken Systemy Antywirusowe jako źródła.
Data udostępnienia: 12.04.2024
Z pozdrowieniami Piotr Rozmiarek
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.