ATAK NA COLONIAL PIPELINE. CYBERPRZESTĘPCY ZAPRZECZAJĄ POWIĄZANIOM Z OBCYM RZĄDEM

W poniedziałek FBI potwierdziło, że odpowiedzialność za cyberatak na sieć największego w USA operatora rurociągów paliwowych Colonial Pipeline spoczywa na grupie DarkSide. Prezydent USA Joe Biden poinformował, że jego administracja ściśle współpracuje z operatorem, aby złagodzić skutki ataku.

„FBI potwierdza, że ransomware DarkSide jest odpowiedzialny za uderzenie na sieć Colonial Pipeline. Kontynuujemy współpracę nad śledztwem z firmą i naszymi partnerami rządowymi” – głosi krótkie oświadczenie Federalnego Biura Śledczego w tej sprawie. Atak DarkSide wstrzymał dostawy paliwa na wschodnim wybrzeżu USA.

"Moja administracja traktuje to bardzo poważnie. FBI i ministerstwo sprawiedliwości podjęło wysiłki, aby powstrzymać i ścigać przestępców ransomware" – mówił Biden wypowiadając się w Białym Domu na temat gospodarki. Jak dodał ministerstwo energetyki współpracuje z firmą, aby rurociąg jak najszybciej zaczął pracować na pełnych obrotach.

„Eksperci od cyberbezpieczeństwa, którzy monitorowali DarkSide, powiedzieli, że wydaje się ona być złożona z weteranów cyberprzestępczości. Koncentrują się na wyciskaniu od swych ofiar jak najwięcej pieniędzy, jak tylko mogą” – podkreśla Reuters. Agencja, powołując się na szefa zajmującej się bezpieczeństwem firmy Cybereason z Bostonu Liora Divę, twierdzi, że grupa jest nowa, ale bardzo dobrze zorganizowana. Sugeruje on, że ataku dokonał ktoś, kto tam (w Colonial Pipeline) był.

"To tak, jakby ktoś włączył przełącznik" - wyjaśniał Div, dodając, że w ciągu ostatnich kilku miesięcy ponad 10 klientów jego firmy odpierało próby włamania ze strony tej grupy. W jego opinii od innych przestępczych grup DarkSide odróżnia praca wywiadowcza poprzedzająca uderzenie.

Zwykle "wiedzą, kto jest menedżerem, wiedzą, z kim rozmawiają, wiedzą, gdzie są pieniądze, wiedzą, kto jest decydentem" – wyliczył Div.

W jego przekonaniu zaatakowanie Colonial Pipeline, z jego potencjalnie ogromnymi konsekwencjami dla Amerykanów na całym wschodnim wybrzeżu, mogło być błędem. "Nie jest to dobre dla ich biznesu, gdy rząd USA angażuje się w sprawę, gdy angażuje się FBI. To ostatnia rzecz, jakiej potrzebują" - argumentował.

Biały Dom ocenił w poniedziałek, że nie ma żadnych problemów z dostawami paliwa. W weekend powołał grupę roboczą do walki z potencjalnymi problemami z dostawami energii. Rozluźnił też przepisy dotyczące transportu autostradami ropy naftowej.

Colonial Pipeline, który dostarcza z rafinerii nad Zatoką Meksykańską do wschodniej i południowej części USA 45 proc. używanych tam paliw, tymczasowo zamknął w piątek swoją sieć rurociągów.

Amerykańskie media zwracają uwagę, że jeśli impas potrwa dłużej wpłynie to na znaczne podwyższenie cen energii.

Według Reutersa DarkSide jest jedną z wielu coraz bardziej sprofesjonalizowanych grup cyfrowych wyłudzaczy, z listą mailingową, centrum prasowym, gorącą linią dla ofiar. Posługuje się nawet rzekomo kodeksem postępowania mającym na celu przedstawienie grupy jako wiarygodnych, choć bezwzględnych, partnerów biznesowych.

„Tacy eksperci jak Div twierdzą, że DarkSide prawdopodobnie składa się z weteranów ransomware'u, pojawiła się znikąd w połowie zeszłego roku i natychmiast rozpętała cyfrową falę przestępczości. Działa poprzez szyfrowanie danych ofiary; zazwyczaj hakerzy oferują ofierze klucz w zamian za płatności w kryptowalutach, które mogą sięgać setek tysięcy, a nawet milionów dolarów. Jeśli ofiara się opiera, aby zwiększyć presję hakerzy coraz częściej grożą wyciekiem poufnych danych” – podała agencja prasowa.

Na swej stronie DarkSide przypomina przeszłe przestępstwa hakerów, twierdząc że zarobiła na tym miliony. Jest tam też galeria wyciekłych danych ofiar, które nie zapłaciły. Obejmuje skradzione dokumenty z ponad 80 firm w całych Stanach Zjednoczonych i Europie.

„Pod pewnymi względami DarkSide jest trudny do odróżnienia od coraz bardziej zatłoczonego pola internetowych wyłudzaczy. (…) wydaje się oszczędzać rosyjskie, kazachskie i ukraińskojęzyczne firmy, co sugeruje związek z byłymi republikami sowieckimi” – ocenił Reuters. Agencja powołuje się na studenta informatyki Georgia Tech, Chuonga Donga, który opublikował analizę programowania DarkSide. Twierdzi on, że wiedza techniczna grupy nie jest niczym szczególnym, a kod DarkSide był "całkiem standardowym ransomware".

Jak zauważył „Wall Street Journal” w poniedziałek, DarkSide zamieścił oświadczenie, twierdząc, że celem grupy jest wyłącznie zarabianie pieniędzy i zaprzeczył związkom z zagranicznym rządem.

"Jesteśmy apolityczni, nie bierzemy udziału w geopolityce. (…) Naszym celem jest zarabianie pieniędzy, a nie tworzenie problemów dla społeczeństwa" – głosi m.in. oświadczenie.

PAP/PAP