JBS recunoaste ca a platit hackerilor o rascumparare de 11 milioane de dolari

Procesatorul de carne JBS USA a platit o rascumparare în bitcoin echivalenta cu 11 milioane de dolari, dupa un atac cibernetic, care a afectat o mare parte dintre operatiunile sale în America de Nord si Australia, a declarat miercuri directorul general al companiei, Andre Nogueira, transmite Reuters.

La începutul acestei luni, grupul brazilian JBS SA, cel mai mare furnizor mondial de carne, a informat ca a fost nevoit sa îsi închida facilitatile de procesare din SUA ca urmare a unui atac organizat al piratilor cibernetici asupra unora dintre serverele sale.

"Aceasta a fost o decizie foarte dificila de luat pentru compania noastra si pentru mine personal. Cu toate acestea, am considerat ca trebuie luata aceasta decizie pentru a preveni orice riscuri potentiale la adresa clientilor nostri", a spus Andre Nogueira, cu privire la decizia JBS de a plati rascumpararea piratilor informatici.

Potrivit unor surse din apropierea acestui dosar, în spatele atacului cibernetic de la JBS s-ar afla un grup de hackeri rusi cunoscut sub denumirea de REvil (Ransomware Evil; de asemenea cunoscut si ca Sodinokibi).

Acest atac a venit la o luna dupa ce compania americana Colonial Pipeline, care detine cea mai importanta retea de conducte petroliere din SUA, a fost vizata si ea de un atac cibernetic care a afectat livrarile de carburanti timp de mai multe zile în zona de sud-est a SUA.

Colonial Pipeline a recunoscut ca a platit o rascumparare de 4,4 milioane de dolari, sau 75 de bitcoini, atacatorilor cibernetici. Cu toate acestea, autoritatile americane au anuntat ulterior ca au recuperat 2,3 milioane de dolari din rascumpararea platita unor hackeri de catre grupul Colonial Pipeline.

"Departamentul Justitiei a localizat si a recuperat majoritatea rascumpararii pe care Colonial a platit-o DarkSide luna trecuta", a declarat luni procurorul general adjunct al SUA, Lisa Monaco, într-o conferinta de presa, referindu-se la reteaua criminala acuzata ca se afla la originea acestei operatiuni de extorcare.

La rândul sau, directorul FBI Christopher Wray a declarat pentru Wall Street Journal ca agentia investigheaza circa 100 de tipuri diferite de atacuri ransomware, din care multe pot fi urmarite pâna la actori din Rusia. Fiecare dintre cele 100 de variante de software malitios este responsabila pentru numeroase atacuri de tip ransomware, a declarat Christopher Wray pentru ziarul citat.

Prin atacurile de tip ransomware datele victimelor sunt criptate. De obicei hackerii ofera victimei atacului o cheie de criptare, în schimbul unor plati în criptomoneda care pot fi de sute de mii sau chiar de milioane de dolari.