

Mysterious cyber attack paralyzes the world's largest meat supplier

A cyber attack forced the world's largest meat supplier - JBS. This forced the JBS company to close some factories in the US, Canada and Australia on June 1-2.

It is not clear which hacker group staged the attack, and there is no information on when the affected facilities in Ottumwa, Iowa will reopen; Worthington, Minnesota; Cactus, Texas; Greeley, Colorado; Brooks, Alberta; and across Australia.

In a press release, JBS USA called the attack an "organized cyber security attack" and said they targeted servers that support information technology systems in North America and Australia.

"The company's backup servers were not affected and an Incident Response company is working to restore the system as soon as possible," JBS USA said. "At this time, the company does not have any evidence that customer, supplier or employee data has been stolen or used for malicious purposes."



JBS is responsible for about 25% of total meat processing in the US and about 20% of total meat processing in Australia. In Australia alone, the company has 47 facilities and about 11,000 employees. The AP quoted an Australian government official as saying it could take several days before production resumed in the country.

Cyberattacks targeting critical infrastructure appear to be on the rise. In May, a group of ransomware took down the Colonial Pipeline and caused a wave of fuel shortages in many parts of the US. This is one of the largest ransomware attacks to date, and it forced the DHS and TSA to impose new guidelines that require pipeline owners to notify federal authorities if they become the victim of an attack. ransomware attack.

You finished reading the article "**Mysterious cyber attack paralyzes the world's largest meat supplier**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.

