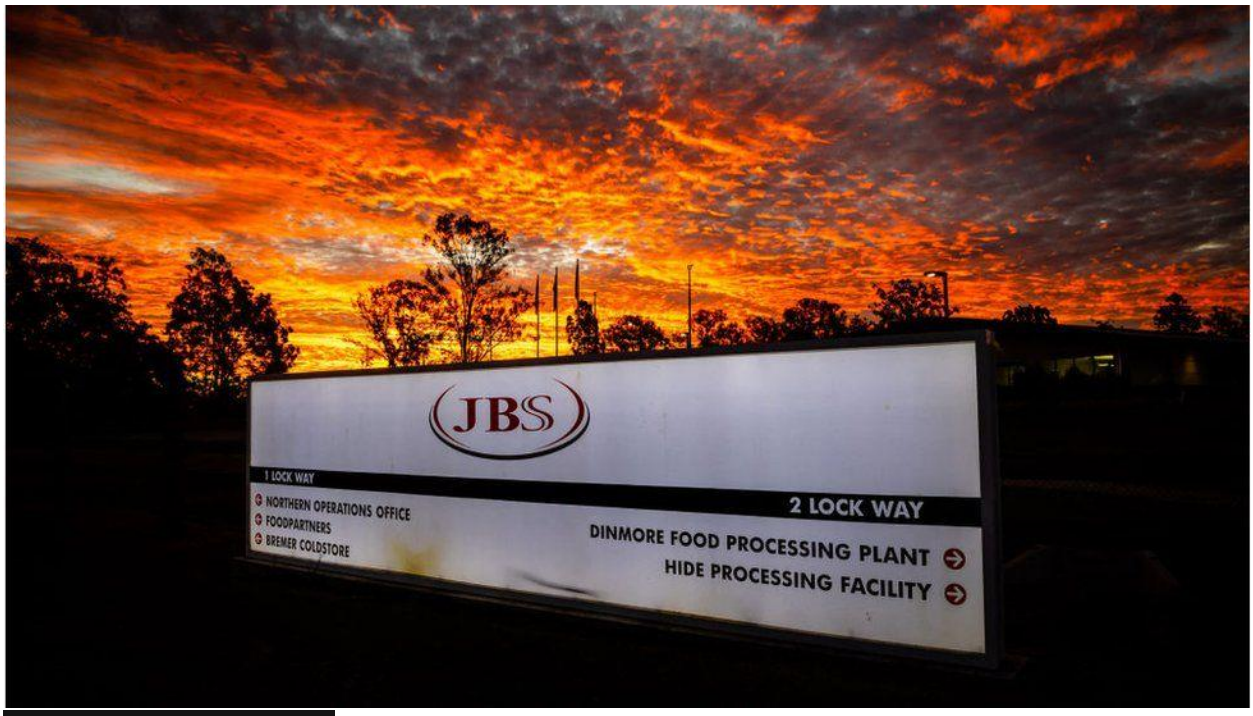
Source (BBC): https://www.bbc.com/news/world-us-canada-57318965

JBS: Cyber-attack hits world's largest meat supplier

Published 2 June 2021



SOURCE,GETTY IMAGES

The world's largest meat processing company has been targeted by a sophisticated cyber-attack.

Computer networks at JBS were hacked, temporarily shutting down some operations in Australia, Canada, and the US, with thousands of workers affected.

The company believes the ransomware attack originated from a criminal group likely based in Russia, the White House said.

The attack could lead to shortages of meat or raise prices for consumers.

In a ransomware attack, hackers get into a computer network and threaten to cause disruption or delete files unless a ransom is paid.

The White House says the FBI is investigating the attack.

"JBS notified [the White House] that the ransom demand came from a criminal organization likely based in Russia," White House spokeswoman Karine Jean-Pierre said on Tuesday.

"The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbour ransomware criminals," she added.

On Wednesday Russia's Deputy Foreign Minister Sergei Ryabkov told local media the Biden administration had been in contact with Moscow to discuss the cyber-attack.

JBS: From regional player to multinational

- JBS is the world's largest meat supplier with more than 150 plants in 15 countries
- It was founded in Brazil in 1953 as a slaughtering business by rancher José Batista Sobrinho
- The company now has more than 150,000 employees worldwide
- Its customers include supermarkets and fast-food outlet McDonald's
- In the US, JBS processes nearly one-quarter of the country's beef and one-fifth of its pork

JBS said **it had made "significant progress" in resolving the cyber-attack** and hoped the vast majority of its plants would be operational on Wednesday.

The company said on Monday that it suspended all affected IT systems as soon as the attack was detected, and that its backup servers were not hacked.

The United Food and Commercial Workers' Union, which represents JBS plant employees, has urged the company to ensure workers still receive their pay.

IT systems are essential in modern meat processing plants, with computers used at multiple stages including billing and shipping.

According to the trade group **Beef Central**, "supermarkets and other large end-users like the McDonald's burger patty supply network will be some of the most immediately impacted customers, due to their need for consistent supply".

JBS's five biggest beef plants are in the US, and the shutdowns have halted a fifth of meat production there, according to Bloomberg.

Plants in Australia and Canada have also been affected but the company's South American operations have not been disrupted.

Last month, fuel delivery in the southeast of the US was crippled for several days after **a ransomware attack targeted the Colonial Pipeline**. Investigators say that attack was also linked to a group with ties to Russia.

Colonial Pipeline has confirmed it paid a $4.4m (£3.1m) ransom to the cyber-criminal gang responsible.

The US government has recommended in the past that companies do not pay criminals over ransomware attacks in case they invite further hacks in the future.

Reference (follow-up): Meat giant JBS pays $11m in ransom to resolve cyber-attack

Meat giant JBS pays $11m in ransom to resolve cyber-attack

Published
10 June 2021

Share

IMAGE SOURCE,GETTY IMAGES

The world's largest meat processing company has paid the equivalent of $11m (£7.8m) in ransom to put an end to a major cyber-attack.

Computer networks at JBS were hacked last week, temporarily shutting down some operations in Australia, Canada and the US.

The payment was reportedly made using Bitcoin after plants had come back online.
JBS says it was necessary to pay to protect customers.
In a ransomware attack, hackers get into a computer network and threaten to cause disruption or delete files unless a ransom in cryptocurrency is paid.

"This was a very difficult decision to make for our company and for me personally," said JBS chief executive Andre Nogueira.

- **US recovers most of Colonial Pipeline ransom**
- **FBI accuses Russia-linked hackers of attack on JBS**
- **Should paying hacker ransoms be banned?**
- **Should firms be more worried about firmware attacks?**

The company added that it paid the money because of the sophistication of the attack, even though the "vast majority" of its plants remained operational.

The company was forced to halt cattle slaughtering at all of its US plants for a day.

That disruption threatened food supplies and risked higher food prices for consumers.

The White House has said that a criminal organization "likely based in Russia" was behind the attack.

Last month, fuel delivery in the southeast of the US was crippled for several days after a ransomware attack targeted the Colonial Pipeline.

Investigators say that attack was also linked to a group with ties to Russia.

Colonial Pipeline has confirmed it paid a $4.4m (£3.1m) in ransom to the cyber-criminal gang responsible.

The Justice Department has recovered some $2.3m.

JBS, a Brazil-based company, said that, "preliminary investigation results confirm that no company, customer or employee data was compromised," in the hack on its systems.

US President Joe Biden is expected to meet his Russian counterpart Vladimir Putin in Geneva next week.

President Biden set off on his first official overseas trip with a warning to Russia that it faces "robust and meaningful" consequences if it engages in "harmful activities".

"The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbour ransomware criminals," A White House spokeswoman said last week.