World's largest meat processor JBS hit by ransomware attack, shutting down US operations

Kevin Reed
2 June 2021

The US beef processing operations of the global meat processing company JBS SA were shut down on Sunday by a ransomware cyberattack. The Brazil-based company is the world's largest processor of beef, chicken and pork products and operates 109 facilities in six countries.

The company confirmed that it had closed its nine beef processing plants in the US, as reported on Tuesday by *Bloomberg*, based on information obtained from an unnamed United Food and Commercial Workers (UFCW) union official.

The company said in a statement on Monday that servers in North America and Australia had been hit by the attack. Reuters reported that the firm halted cattle slaughter in the US and shut down its operations in Australia.

A company representative in Sao Paolo said that its Brazilian operations were not impacted by the hack. JBS Canada reported on its Facebook page that it operated late shifts on Tuesday at its beef plant in Brooks, Alberta after shutting down shifts earlier in the day and on Monday.

JBS issued a statement that the company took immediate action, "suspending all affected systems, notifying authorities and activating the company's global network of IT professionals and third-party experts to resolve the situation." The company said its backup servers were not affected and is "actively working with an Incident Response firm to restore its systems as soon as possible."

Ransomware attacks typically involve remote encryption of all data on host computers combined with messaging that demands a sum of money—often in cybercurrency in the thousands or millions of dollars—in exchange for the decryption key required to restore operational control of the systems.

John Hultquist of the security and government consulting firm FireEye told Reuters, "The supply chains, logistics and transportation that keep our society moving are especially vulnerable to ransomware, where attacks on chokepoints can have outsized effects and encourage hasty payments" to the hackers.

Aboard Air Force One, Biden administration officials were quick to blame Russia for the ransomware attack on JBS without providing any facts or evidence to prove the assertion. White House principal deputy press secretary Karine Jean-Pierre told reporters, "JBS notified the administration that the ransom demand came from a criminal organization, likely based in Russia." Jean-Pierre added, "The White House is engaging directly with the Russian government on this matter and delivering the message that responsible states do not harbor ransomware criminals."

The details of JBS SA's response to the attack, whether the company paid the ransom or not, are unknown at this time. The company is working with the FBI and the Cybersecurity and Infrastructure Security Agency to investigate the breach and provide technical support. Jean-Pierre told reporters, "The White House has offered assistance to JBS, and our team and the Department of Agriculture have spoken to their leadership several times in the last day."

JBS SA, with its US operations based in Greeley, Colorado, became the world's largest meat processor through a series of mergers and acquisitions that included Swift & Company (2007), Smithfield Foods (2008), Pilgrim's Pride (2009) and the pork processing

business of Cargill Meat Solutions (2015). It has more than $50 billion in annual sales worldwide and the company employs approximately 25,000 workers in the US.

JBS is notorious for its response to the COVID-19 pandemic, forcing meatpacking workers to stay on the job throughout as part of the “essential workforce.”

With an estimated 20 percent of meatpacking workers contracting the virus and hundreds who have died from it, JBS used intimidation and lies to conceal the extent of infection and keep sick workers on the job during the pandemic. The company relied on its partner in the UFCW to suppress worker opposition that found expression over the last year in multiple wildcat walkouts and protests in defiance of the union bureaucracy across the country.

Company CEO Andre Nogueira sent a message to *USA Today* on Tuesday saying that “the vast majority of our beef, pork, poultry and prepared foods plants will be operational tomorrow.” Clearly concerned about the impact of the cyberattack on its market position—JBS has a Wall Street value of $76+ billion—Nogueira said, “Our systems are coming back online, and we are not sparing any resources to fight this threat. We have cybersecurity plans in place to address these types of issues and we are successfully executing those plans.”

Industry analysts reported that US meatpackers slaughtered 22 percent fewer cattle than a week earlier and 18 percent than a year earlier, according to estimates from the US Department of Agriculture. Pork processing was also down. Prices for choice and select cuts of US beef shipped to wholesale buyers each jumped more than 1 percent.

The JBS attack happened a few weeks after a similar ransomware breach of the Colonial Pipeline network that shutdown a major artery of refined petroleum product transport to the eastern and southeastern sectors of the US from Texas. In that attack, the FBI claimed a “criminal group” called DarkSide located in Russia was responsible. The Kremlin publicly denied any connection to the hack.

On May 11, Dmitry Peskov, a spokesman for Russian President Vladimir Putin, told US reporters, “Russia has nothing to do with these hacker attacks, and had nothing to do with the previous hacker attacks,” referring to the Colonial Pipeline incident and the SolarWinds hack in late March that compromised nine federal agencies and more than 100 private sector groups for a year by exploiting vulnerabilities on Microsoft's Exchange Server. Peskov added, “We categorically do not accept any accusations against us.”

The FBI released a statement late Wednesday declaring that its investigation had determined the hack had been carried out by groups known as REvil and Sodinokibi and that the agency is “working diligently to bring the threat actors to justice.”

While the FBI did not mention any connection between these groups and Russia, it is widely known in cybersecurity circles that they are thought to be based in the country even though their exact location cannot be precisely identified. In some instances, the two names are joined into one as REvil/Sodinokibi and refer to a specific kind of ransomware discovered in 2019 that is based on the code of a malware platform called GandCrab that uses the ransomware-as-a-service (RaaS) model.

The timing of the JBS cyberattack coincidentally corresponds with the political agenda of the Biden White House as the president prepares for a summit with Putin scheduled for June 16 in Geneva. Biden Press Secretary Jen Psaki said during a press briefing on Wednesday that the administration is not “taking any options off the table” in responding to the JBS attack. Psaki added, “I'm not going to give any further analysis on that. Other than to tell you that our view is that when there are criminal entities within a country, they certainly have a responsibility, and it is a role that the government can play.”

Later in the afternoon, when President Joe Biden was asked if the US would retaliate against Russia for the attack, he said, “We’re looking closely at that issue.”