kindred

Security Newsletter

7 Jun 2021

Subscribe to this newsletter

Ransomware Hits a Food Supply Giant

Hackers targeting JBS USA have disrupted meat processing facilities around the world, just one month after the Colonial Pipeline attack caused fuel distribution havoc.

JBS SA is the world's largest meat processing company, with headquarters in Brazil and more than 250,000 employees worldwide. In a statement on Monday, its American subsidiary, JBS USA, said that "it was the target of an organized cybersecurity attack, affecting some of the servers supporting its North American and Australian IT systems."

The company added that its system backups are intact. In response to the attack, JBS USA took impacted systems offline, notified law enforcement, and began working with an outside incident response firm on remediation. JBS facilities in Australia, the US, and Canada have faced disruptions since the attack was first detected on Sunday.

Read More on Wired

More #News

- Amazon to share your Internet with neighbors on Tuesday
- Norton 360 antivirus now lets you mine Ethereum cryptocurrency
- Swedish Health Agency shuts down SmiNet after hacking attempts
- Microsoft Teams calls are getting end-to-end encryption in July
- Firefox now blocks cross-site tracking by default in private browsing
- Breached companies facing higher interest rates and steeper collateral requirements
- GitHub Updates Policy to Remove Exploit Code When Used in Active Attacks
- Google Chrome now warns you of extensions from untrusted devs
- EU Adopts New Privacy-Focused Data Sharing Tools
- Inside The 'World's Largest' Video Game Cheating Empire

- Inside The 'World's Largest' Video Game Cheating Empire
- Report: Danish Secret Service Helped NSA Spy On European Politicians

#Breach Log

- Fujifilm confirms ransomware attack disrupted business operations
- Meat giant JBS now fully operational after ransomware attack
- UF Health Florida hospitals back to pen and paper after cyberattack
- Chinese threat actors hacked NYC MTA using Pulse Secure zero-day
- Massachusetts' largest ferry service hit by ransomware attack
- US Justice Department accuses Latvian national of deploying Trickbot malware

#Patch Time!

- Critical WordPress plugin zero-day under active exploitation
- 10 Critical Flaws Found in CODESYS Industrial Automation Software
- Hackers Actively Exploiting 0-Day in WordPress Plugin Installed on Over 17,000 Sites
- A New Bug in Siemens PLCs Could Let Hackers Run Malicious Code Remotely
- Overwolf 1-Click Remote Code Execution

#Tech and #Tools

- XSS in the AWS Console
- Kali Linux 2021.2 Release
- reqstress - a benchmarking&stressing tool
- WE.LOCK: Unlocking Smart Locks with Web Vulnerabilities
- iOS User Enrollment and Trusted Certificates
- ASP.NET Cryptography for Pentesters
- UI Security - Thinking Outside the Viewport
- XSS vulnerability found in popular WYSIWYG website editor
- SharpPanda: Chinese APT Group Targets Southeast Asian Government With Previously Unknown Backdoor
- OSX/Hydromac: A new macOS malware leaked from a Flashcards app
- Grav CMS 1.7.10 - Code Execution Vulnerabilities

This content was created by Kindred Group Security. Please share if you enjoyed!

Kindred Group in brief

Kindred Group is one of the world's leading online gambling operators with business across Europe, US and Australia, offering 30 million customers across 9 brands a great form of entertainment in a safe, fair and sustainable environment. The company, which employs about 1,600 people, is listed on Nasdaq Stockholm Large Cap and is a member of the European Gaming and Betting Association (EGBA) and founding member of IBIA (Sports Betting Integrity Association). Kindred Group is audited and certified by eCOGRA for compliance with the 2014 EU Recommendation on Consumer Protection and Responsible Gambling (2014/478/EU). Read more on www.kindredgroup.com.

You can access the previous newsletters at https://news.infosecgur.us