Security News Blog Post
Selected Topic: JBS Ransomware Attack
Group Members: Seungwon Burm, Yuchan Kim, Jeong Yong Yang, Cristobal Newman

Abstract

JBS is a large-scale meat provider company that processes, packs, and transports meat and poultry products to customers in more than 100 countries [12]. JBS USA is the largest company in JBS, consisting of JBS USA Beef, JBS USA Pork, JBS USA Live Pork, JBS USA retail ready, JBS USA carrier, and Plumrose USA [12].

JBS became the target of a cybersecurity attack on May 30, 2021, which affected servers in North America and Australia [13]. The attack forced JBS to pause the operating system, which delayed the transactions while resolving the situation [13]. This ransomware attack on JBS is the focus of the blog post.

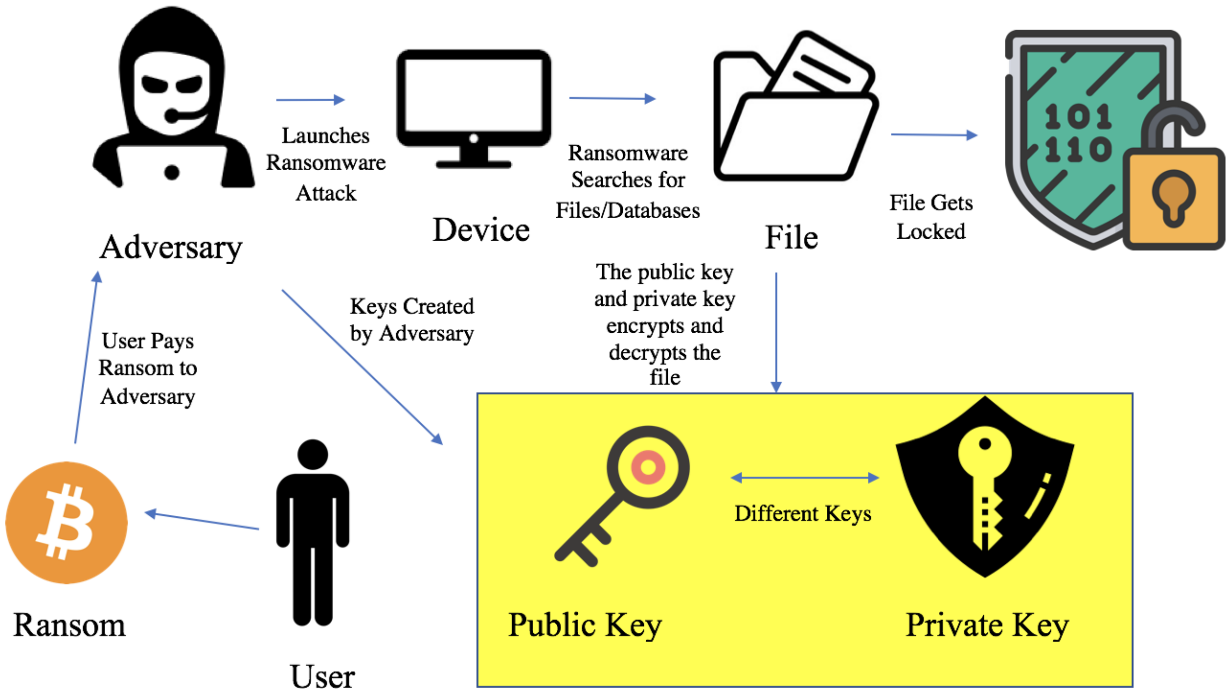
Despite the large-scale attack that led JBS to shut down for four days, only limited information exists on how the attack was launched. In this report, we provide how ransomware attacks work and possible suggestions on how to avoid ransomware attacks. In addition, we will provide the effect of the attack and the legal and ethical issues raised by the attack.

What is Ransomware Attack?

Ransomware is malicious software that prevents access to information until a ransom is paid [1]. In other words, databases, files, or applications that include crucial information regarding users and organizations are encrypted [1]. Attacks using ransomware have got popular for a few reasons: “easy availability of malware kits that can be used to create new malware” [1], “use of known good generic interpreters to create cross-platform ransomware” [1], and “use of new techniques, such as encrypting the complete disk instead of selected files” [1]. In addition, the usage of cryptocurrency, such as Bitcoin, to provide and receive ransom makes it difficult for the FBI and organizations to track down criminals by following the money trail [1]. Therefore, the easy accessibility of a powerful attack combined with the security of the criminals and the large amount of money they can receive as ransom contributes to the widespread use of ransomware to launch attacks on organizations.

How Ransomware Works

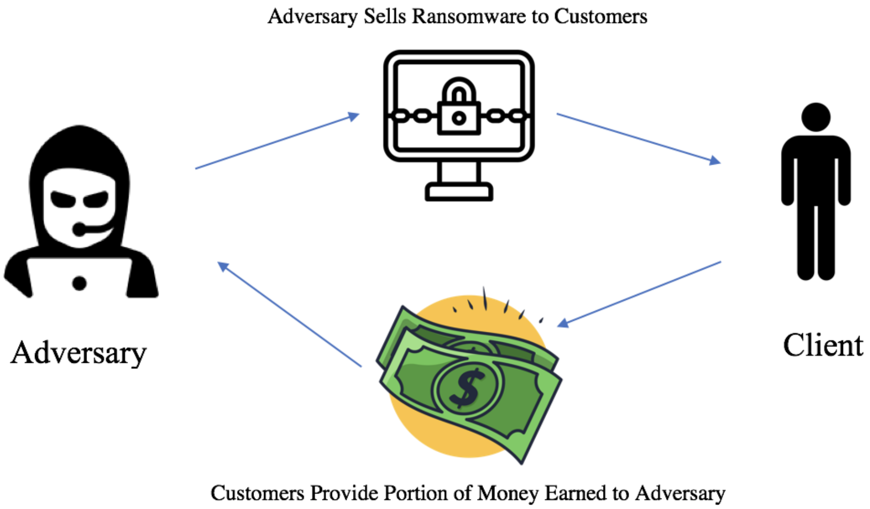
Ransomware uses asymmetric encryption, the usage of a pair of keys to encrypt and decrypt the file [1]. Once attacks using ransomware are successfully launched on users and organizations, the files/servers/databases that belong to them will be locked with the public-private pair of keys created by the adversary [1]. Since users and organizations cannot decrypt the files without knowing the private key, they are forced to pay ransom to the adversaries, who provide the private key to decrypt the files in return [1].


Adversary
Launches Ransomware Attack
Device
Ransomware Searches for Files/Databases
File
File Gets Locked
101
110
Keys Created by Adversary
The public key and private key encrypts and decrypts the file
User Pays Ransom to Adversary
Different Keys
Public Key
Private Key
Ransom
User

There exist many different types of ransomware attacks. The most common attack is malware distribution using email spam [1]. The malware requires "an attack vector to establish its presence on an endpoint" [1]. It stays on the system to damage the files after the presence is established by dropping and executing malicious binary on the device [1]. The binary discovers valuable files and databases and encrypts them using the public-private pair of keys [1]. The vulnerability of ransomware comes from the fact that it can spread quickly over other systems with the infection on one of the servers [1]. In other words, a ransomware attack on one device of the organization could lead to further attacks on the entire organization. If the organization or users fail to back up their servers or system, they are required to pay a ransom to protect and recover their data [1].

Technical Issues

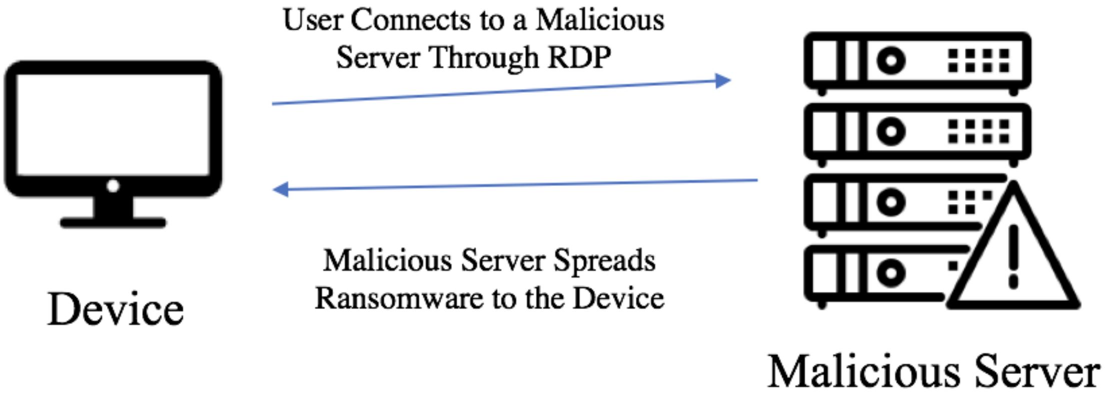
According to the FBI, REvil, the criminal network of ransomware hackers founded in 2019 mostly consisting of Russian members, was behind the attack [4]. REvil is known to operate using ransomware-as-a-service (RAAS) enterprise, a subscription-based model that allows adversaries to use previously developed ransomware [4]. The malware developers create malware and sell it to customers, who attack a server or organization and pay the developers a percentage of the money earned through the attack [4], [5]. This type of attack benefits both the customers and the developers since customers who do not have any knowledge or skill can launch the ransomware attack while developers take fewer risks since they do not directly damage the organizations [1], [5].


Adversary Sells Ransomware to Customers
Adversary
Client
Customers Provide Portion of Money Earned to Adversary

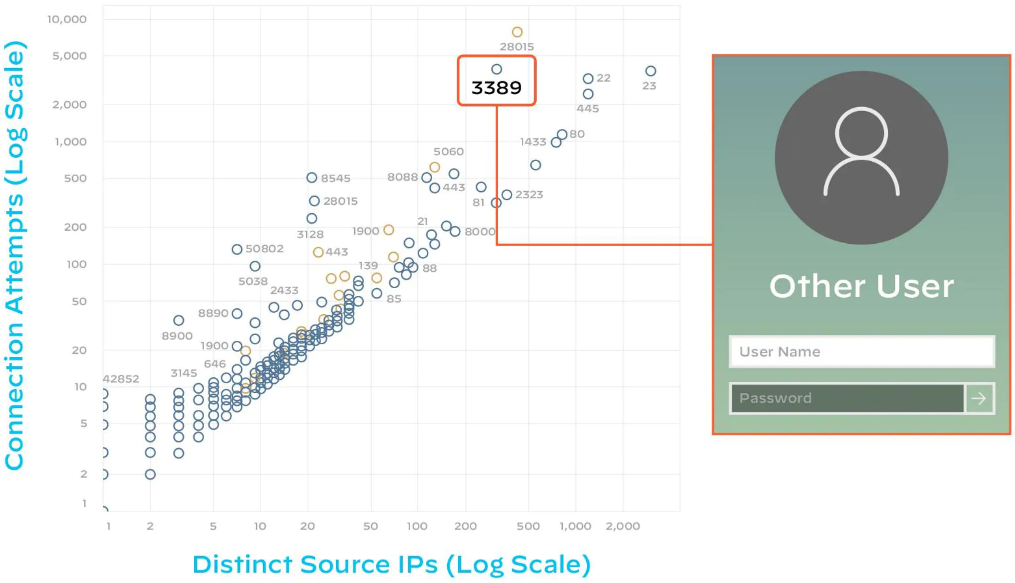
Although the exact method REvil used to launch ransomware attacks onto JBS servers is unknown, the adversaries likely used remote access protocols from the information that it is one of the most famous methods of ransomware intrusions and that there exist failure connection attempts using Remote Desktop Protocol (RDP) connection to JBS Australia IP address space on February 28, 2021 [6]. This indicates that the adversaries checked whether there exists an RDP service running on JBS through the RDP request [6]. With the information that REvil eventually breached data from JBS Australia and Brazil (discussed in the impact session), we assumed that REvil continued to use RDP as a tool to launch ransomware attacks to JBS USA and Canada as well.

RDP allows people to connect to the faraway desktop computer from a separate computer [22]. Users can access the desktop computer to manipulate files and use applications as if they are actually working on the desktop computer through the usage of RDP, which is beneficial when working at home or from other remote locations [22]. The RDP protocol opens a network channel that sends data between the connected devices through the usage of port 3389 [22]. The actions that users take on the remote computer, such as mouse movements, keystrokes, etc. are transmitted to their desktop computer over the internet via TCP/IP and provides security by encrypting the data sent [22].

There are many possible methods for launching RDP ransomware attacks. One of the popular methods for exploiting RDP is through the usage of a “reverse” RDP attack, which can be done by adversaries infecting a server with malware [3]. When an off-site employee connects to the online server infected by malware using RDP, adversaries can gain access to the offsite device by traversing the RDP connection, which can lead to ransomware attacks on the specific device [3]. The vulnerability of the “reverse” RDP ransomware attack comes from the fact that every client that connects to the server can be affected by ransomware and that it can spread to other devices from the infection of a device, as mentioned above [3]. This method is known as a “reverse” RDP attack since it is not the traditional way of infected clients affecting the server but is the infected server attacking the visitors of the server [3].


User Connects to a Malicious Server Through RDP
Device
Malicious Server Spreads Ransomware to the Device
Malicious Server

Another popular RDP ransomware attack is through the usage of port 3389, which is used by all RDPs as the default listening port [2], [7]. Since the port number is public and known to everybody, attackers can scan the internet for an open port 3389 by using a Nmap script on the internet [7]. In fact, searching the whole internet for port 3389 can be done in 45 minutes, which is a fast speed [7]. Once unclosed port 3389s are found, adversaries can get into the server to launch ransomware attacks by learning the login credentials, which can be done by social engineering, brute force attacks, man-in-the-middle attacks, etc [2], [7].



(Image from https://www.paloaltonetworks.com/blog/2021/07/diagnosing-the-ransomware-deployment-protocol/)

Prevention

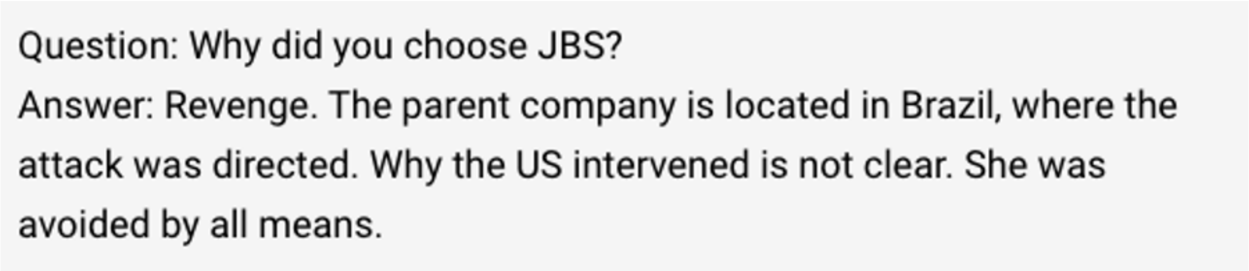
Since it is unknown how REvil launched its ransomware attack on the server of JBS, providing specific advice on how the attack could be prevented is difficult. With the information that the attack was performed through the usage of ransomware, these are some of the general advice on how to prevent ransomware attacks in general: backing up of the data since the backup allows the organization or users to preserve important files so that they can simply reinstall the backup files even if their data is locked and safe surfing and using secure networks by not responding to malicious or suspicious emails and text messages and downloading trustable applications [1]. In addition, the securing of the backup data in different locations is very significant since the malware can navigate through the server to also lock the backup data, which can lead to the loss of the backup data as well [1]. In fact, one of the reasons why JBS was able to recover quickly from the attack was through the backup files that they preserved [8].

In addition, some of the good security practices to protect against the attack through RDP ransomware are making the steps to log in with stolen credentials difficult by using a strong password that prevents dictionary attacks, enabling multi-factor authentication (MFA), limiting access on the RDP by ensuring RDP access is turned off or using allow-list to limit access to only approved IP addresses that can connect to the RDP server, and securing the RDP ports by ensuring that the RDP ports are closed to the internet because RDP ransomware attacks are only available when the RDP is left open [2].

Finally, the reverse RDP ransomware attack could be prevented by keeping the RDP servers updated, never connecting to the RDP server that is not updated nor secured, disabling “bi-directional clipboard sharing to close off any potential vulnerability related to cutting and pasting data between client and server” [3], and monitoring RDP with security tools by using “IDS (intrusion detection system), endpoint protection solution, and threat emulation” [3].

Motivation

The motivation for the ransomware attack on JBS is revealed from an interview with an individual representing REvil, who discussed the attack on the telegram Dark Web Channel known as RUSSIAN OSINT [6]. According to the interview, the attack was intended to target Brazil, where the parent company is located, for revenge [6]. However, the specifics of the revenge, such as the event that led to its decision to attack JBS for revenge, are not stated in the interview. In addition, considering that most of the damage occurred within the United States, Australia, and Canada, whether the target of the attack was truly Brazil is questionable.



Question: Why did you choose JBS?
Answer: Revenge. The parent company is located in Brazil, where the attack was directed. Why the US intervened is not clear. She was avoided by all means.

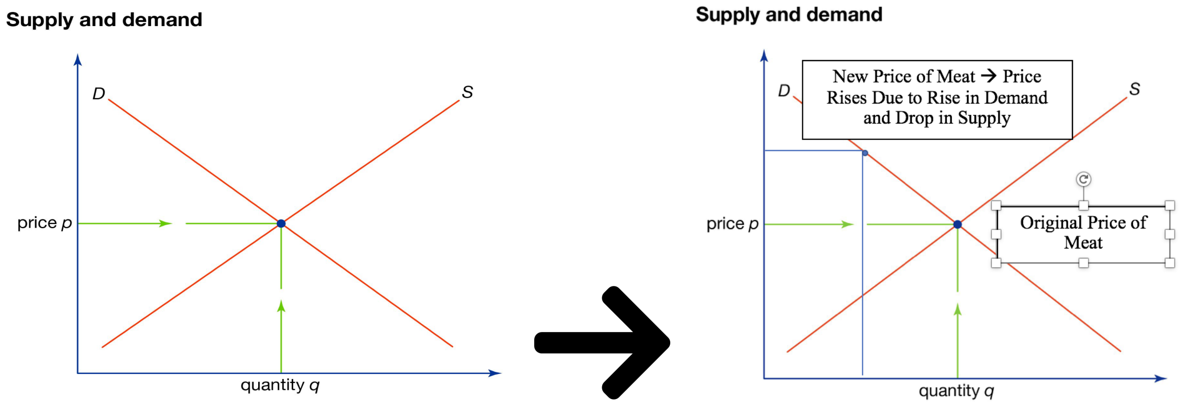
(Image from https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march)

Impact of Attack

Due to the fact that JBS is a worldwide company, the ransomware attack affected countries all over the globe. On May 30, 2021, JBS Australia was the first target, resulting in the leakage of approximately 45 Gigabytes of data into a file-sharing website called 'Mega' [6]. A further attack was observed in JBS Brazil afterward, which also resulted in the upload of the data to Mega [6]. Furthermore, a potential loss of 5 TB of data exfiltration was observed to Mega and other malicious IP addresses in Hong Kong that are not associated with JBS [6]. The ransomware attack forced JBS to temporarily shut down all beef plants in the United States and a beef plant in Canada from May 30, 2021, to June 2, 2021 [14]. As the meat processing plants were closed, the process of killing beef and lamb also paused in Australia [14].

The ransomware attack that led to the temporal shutdown of JBS affected other people. For instance, farmers were required to search for other buyers as JBS no longer needed to purchase goods from them during the shutdown period [15]. The task to find other purchasers was challenging since the market experienced a high supply of products but a lower demand for them, which resulted in the reduction of the price of their products [15]. The restaurants were also categorized as victims of the ransomware attack since they needed to search for alternative suppliers other than JBS [15]. Therefore, many restaurants had to outbuy supplies since they were afraid of the potential rise in the price of meat [15].

The effect of the ransomware attack on JBS on the economic market was non-negligible. As JBS temporarily closed its operations, the demand for meat increased while the supply of it decreased, which resulted in an increase in meat prices during the period. The Food and Agriculture Organization of the United Nations (FAO) published a report regarding food prices on June 1, 2021, which stated that the disruption of JBS operations contributed to the highest peak of meat prices in May 2021 since September 2011 [16].

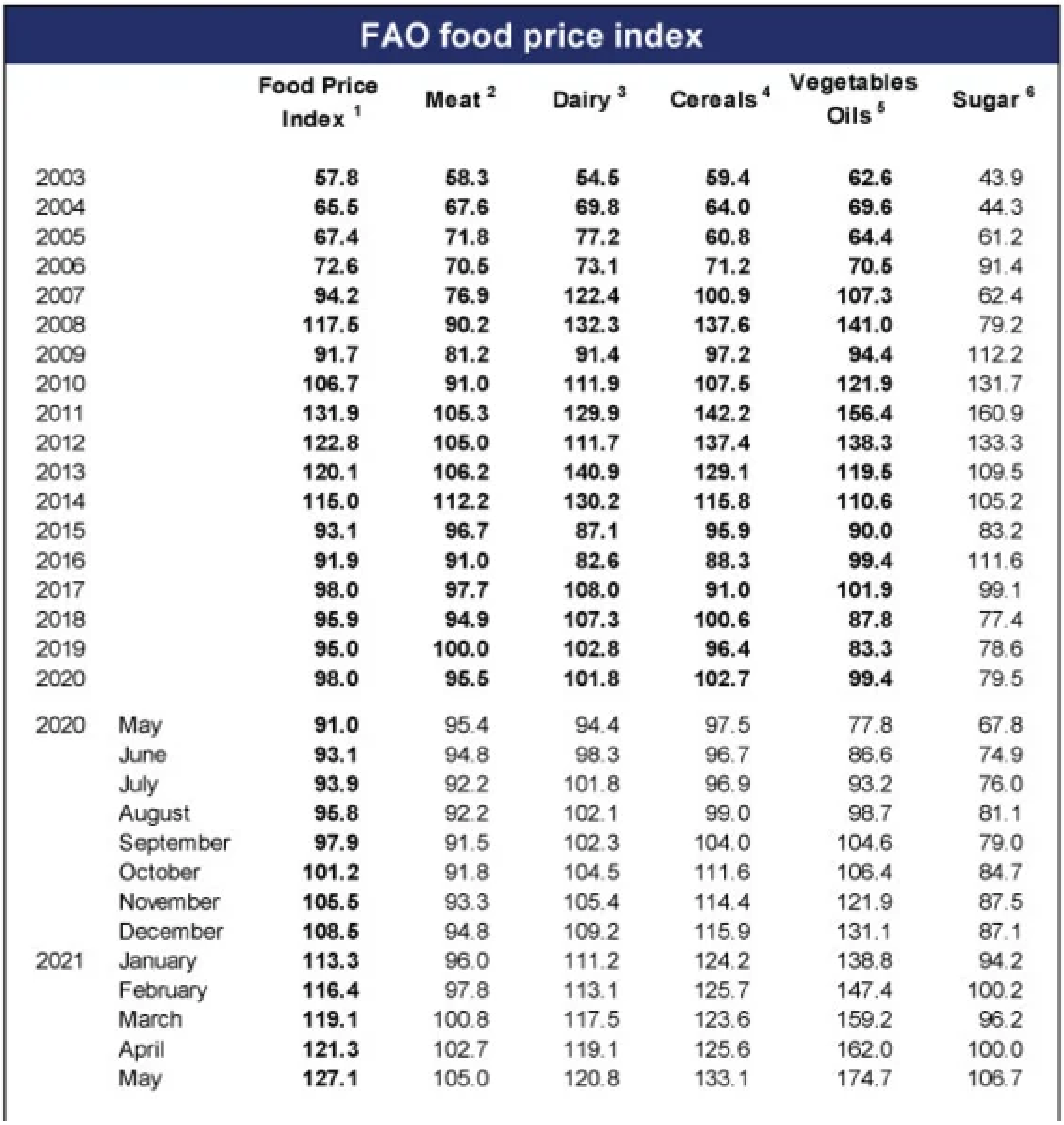


Supply and demand

Supply and demand

New Price of Meat → Price Rises Due to Rise in Demand and Drop in Supply

Original Price of Meat



FAO food price index

		Food Price Index [1]	Meat [2]	Dairy [3]	Cereals [4]	Vegetables Oils [5]	Sugar [6]
2003		**57.8**	**58.3**	**54.5**	**59.4**	**62.6**	43.9
2004		**65.5**	**67.6**	**69.8**	**64.0**	**69.6**	44.3
2005		**67.4**	**71.8**	**77.2**	**60.8**	**64.4**	61.2
2006		**72.6**	**70.5**	**73.1**	**71.2**	**70.5**	91.4
2007		**94.2**	**76.9**	**122.4**	**100.9**	**107.3**	62.4
2008		**117.5**	**90.2**	**132.3**	**137.6**	**141.0**	79.2
2009		**91.7**	**81.2**	**91.4**	**97.2**	**94.4**	112.2
2010		**106.7**	**91.0**	**111.9**	**107.5**	**121.9**	131.7
2011		**131.9**	**105.3**	**129.9**	**142.2**	**156.4**	160.9
2012		**122.8**	**105.0**	**111.7**	**137.4**	**138.3**	133.3
2013		**120.1**	**106.2**	**140.9**	**129.1**	**119.5**	109.5
2014		**115.0**	**112.2**	**130.2**	**115.8**	**110.6**	105.2
2015		**93.1**	**96.7**	**87.1**	**95.9**	**90.0**	83.2
2016		**91.9**	**91.0**	**82.6**	**88.3**	**99.4**	111.6
2017		**98.0**	**97.7**	**108.0**	**91.0**	**101.9**	99.1
2018		**95.9**	**94.9**	**107.3**	**100.6**	**87.8**	77.4
2019		**95.0**	**100.0**	**102.8**	**96.4**	**83.3**	78.6
2020		**98.0**	**95.5**	**101.8**	**102.7**	**99.4**	79.5
2020	May	**91.0**	95.4	94.4	97.5	77.8	67.8
	June	**93.1**	94.8	98.3	96.7	86.6	74.9
	July	**93.9**	92.2	101.8	96.9	93.2	76.0
	August	**95.8**	92.2	102.1	99.0	98.7	81.1
	September	**97.9**	91.5	102.3	104.0	104.6	79.0
	October	**101.2**	91.8	104.5	111.6	106.4	84.7
	November	**105.5**	93.3	105.4	114.4	121.9	87.5
	December	**108.5**	94.8	109.2	115.9	131.1	87.1
2021	January	**113.3**	96.0	111.2	124.2	138.8	94.2
	February	**116.4**	97.8	113.1	125.7	147.4	100.2
	March	**119.1**	100.8	117.5	123.6	159.2	96.2
	April	**121.3**	102.7	119.1	125.6	162.0	100.0
	May	**127.1**	105.0	120.8	133.1	174.7	106.7

(Image from https://fluidattacks.com/blog/jbs-revil-cyberattack/)

Even though JBS did not officially publish the revenue loss from the attack, we can approximately guess the loss from its annual report, which includes the annual revenue of the company. According to its website, JBS stated that its revenue in the United States in 2021 was approximately 27.8 billion dollars [17]. Assuming that JBS sold the same amount of meat and earned the same revenue every day in 2021, it had about 27.8 billion dollars / 361 days (which is 365 days subtracted by four days of shutdown) = 77 million dollars of revenue per day. Therefore, without the shutdown of JBS, it could have earned additional 308 million dollars (77 million dollars * 4 days).

Responses From the Attack

JBS

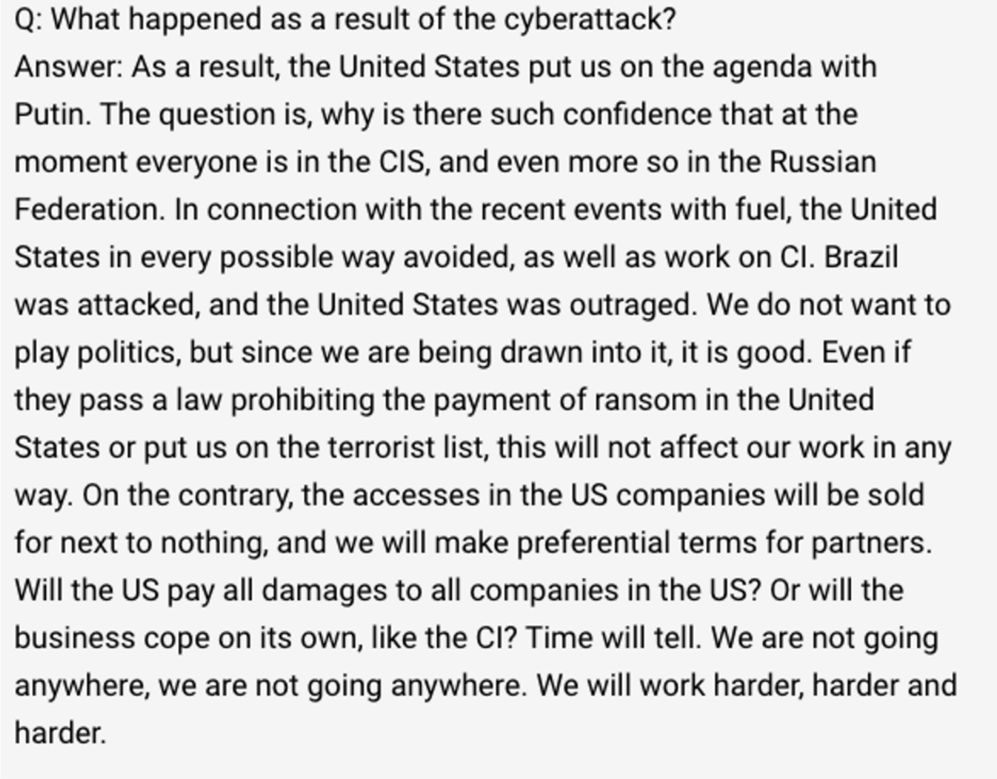
JBS responded to the ransomware attack by suspending systems that were affected, contacting law enforcement and 3rd party consultants for resolving the attack, and communicating with consumers by updating their status daily [8].

- On June 1st, 2021, JBS notified that it was able to bring back its online systems and ship products from its plants to the customers [8]
- On June 2nd, 2021, JBS informed that most of the systems were recovered from the attack and it reopened all of the facilities [8]
- On June 3rd, 2021, JBS USA CEO Andre Nogueira mentioned that the company was able to recover quickly with help from government entities and consultants [8]. He also stated that the adversaries were unable to damage the core JBS systems [8].

Even though JBS announced that its backup systems were undamaged and none of the data was breached by the ransomware attack, it paid 11 million dollars to the adversaries to prevent any potential risk to its customers [18]. However, the report that none of the data from JBS was breached contradicts the report by SecurityScorecard, which states that JBS Australia and Brazil experienced data exfiltration [6]. In addition, the report also mentioned that JBS could have experienced approximately 5 TB of data exfiltration [6].

REvil

An individual representing REvil on the telegram Dark Web Channel called RUSSIAN OSINT mentioned in an interview that even though he/she does not understand why the United States became upset regarding the attack, REvil is satisfied with the unexpected attention from the politicians [6]. Despite getting a large amount of attention, REvil strongly stated that it does not care whether the United States passes a law that would ban the payment for ransomware attacks or not because the group will continue to launch attacks to spread ransomware in the future [6]. The individual also noted that REvil could potentially sell the access of the US companies to its partners if the payment for ransomware becomes prohibited [6].



Q: What happened as a result of the cyberattack?
Answer: As a result, the United States put us on the agenda with Putin. The question is, why is there such confidence that at the moment everyone is in the CIS, and even more so in the Russian Federation. In connection with the recent events with fuel, the United States in every possible way avoided, as well as work on CI. Brazil was attacked, and the United States was outraged. We do not want to play politics, but since we are being drawn into it, it is good. Even if they pass a law prohibiting the payment of ransom in the United States or put us on the terrorist list, this will not affect our work in any way. On the contrary, the accesses in the US companies will be sold for next to nothing, and we will make preferential terms for partners. Will the US pay all damages to all companies in the US? Or will the business cope on its own, like the CI? Time will tell. We are not going anywhere, we are not going anywhere. We will work harder, harder and harder.

(Image from https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march)

Politicians

Politicians also responded to the JBS ransomware attack. Carolyn Maloney, an American politician, mentioned that the decision for JBS to pay $11 million to the adversaries may incentivize further ransomware attacks and insisted that Congress should make laws regarding ransomware activities in the US [20]. Joe Biden declared that Vladimir Putin should take actions to prevent cyberattacks from Russia [21]. Biden warned that the US could potentially shut down the servers of the adversaries if no action is taken from Russia regarding these cyberattacks [21]. President Putin responded that he is willing to help prevent ransomware attacks once the US provides information regarding the adversaries to them [21].

Ethical and Legal Issues

The JBS cyberattack raised the issue of the role of Russia in ransomware attacks against the United States. While there is no evidence that Russia benefits financially from these crimes, President Joe Biden confronted President Vladamir Putin of Russia on the harboring of ransomware criminals who US Officials sometimes claim to have worked for Kremlin security services [11]. The arrest of 14 members of the REvil crime organization has laid some of this speculation to rest [9], [10]. However, the move came at a strange time as debates between the US and Russia were getting more heated over the situation in Ukraine [10]. Vladimir Putin has cited the request of Joe Biden as the reason for the move against REvil, but it is unclear whether it was an act in a good faith or some sort of political ploy [10]. The general rule of thumb in

Russia up to this point has been to turn a blind eye to ransomware criminals unless they attack domestic operations or allied nations, so we have to see if this continues to be the status quo [10].

The JBS cyberattack also brings into perspective the entire U.S. Business infrastructure with regard to cybersecurity. For example, “Critical U.S. infrastructure might be better hardened against ransomware attacks were it not for the 2012 defeat of legislation that would have set cybersecurity standards for critical industries” [11]. The U.S. Chamber of Commerce and other business interests lobbied hard against this bill, indicating that it interfered with normal business operations [11]. Until June 2021, the US had no cybersecurity requirements for businesses outside of the banking, electric, and nuclear field [11]. David White, the president of the cyber risk management company Axio, said that the regulation could help, especially those companies with inadequate cybersecurity programs [11]. JBS may fall into this category as it is the largest food company of at least 40 other food companies that have been targeted by ransomware in the past year leading up to the attack [11]. He also stated, however, that there could be involuntary negative effects with companies seeing the regulations as a ceiling for their cybersecurity program rather than the ground to build off of [11].

Finally, the JBS ransomware attack brings the question of what proper practices concerning ransomware attacks should be. The decision of JBS to pay REvil a sum equivalent to 11 million dollars to further protect its customers will only show ransomware attackers that critical infrastructure in the United States is a target that pays money, which may lead to more attacks in the future.

This work was done without any outside collaboration.

Works Cited

1. https://www.trellix.com/en-us/security-awareness/ransomware/what-is-ransomware.html
2. https://rhisac.org/ransomware/remote-desktop-protocol-use-in-ransomware-attacks/
3. https://ransomware.org/blog/rdp-ransomware-everything-you-need-to-know/
4. https://www.bbc.com/news/world-us-canada-57338896
5. https://www.upguard.com/blog/what-is-ransomware-as-a-service
6. https://securityscorecard.com/blog/jbs-ransomware-attack-started-in-march
7. https://www.paloaltonetworks.com/blog/2021/07/diagnosing-the-ransomware-deployment-protocol/
8. https://www.cshub.com/attacks/articles/iotw-jbs-recovers-quickly-from-a-ransomware-attack
9. https://www.bbc.com/news/technology-59998925
10. https://www.cpomagazine.com/cyber-security/14-members-of-revil-ransomware-gang-arrested-in-russia/
11. https://www.npr.org/2021/06/03/1002819883/revil-a-notorious-ransomware-gang-was-behind-jbs-cyberattack-the-fbi-says
12. https://sustainability2019.jbssa.com/chapters/who-we-are/about-our-company/
13. https://jbsfoodsgroup.com/articles/jbs-usa-cyberattack-media-statement-may-31-most-recent-update
14. https://www.vox.com/recode/2021/6/1/22463179/jbs-foods-ransomware-attack-meat-hackers
15. https://www.wsj.com/articles/ransomware-attack-roiled-meat-giant-jbs-then-spilled-over-to-farmers-and-restaurants-11623403800
16. https://fluidattacks.com/blog/jbs-revil-cyberattack/
17. https://www.zippia.com/jbs-usa-careers-28000/revenue/
18. https://www.nytimes.com/2021/06/09/business/jbs-cyberattack-ransom.html
19. https://www.afr.com/politics/russia-under-fire-as-ransomware-attack-leaves-7000-out-of-work-20210602-p57xha
20. https://thehill.com/policy/finance/557975-oversight-chief-presses-jbs-on-why-it-paid-ransom-amid-cyber-attack/
21. https://apnews.com/article/joe-biden-europe-technology-government-and-politics-russia-df7ef73f02bcba61ad6e628aa95a9f84
22. https://www.cloudflare.com/learning/access-management/what-is-the-remote-desktop-protocol/