CAROLYN B. MALONEY, NEW YORK
CHAIRWOMAN

ONE HUNDRED SEVENTEENTH CONGRESS

JAMES COMER, KENTUCKY
RANKING MINORITY MEMBER

Congress of the United States
House of Representatives
COMMITTEE ON OVERSIGHT AND REFORM
2157 RAYBURN HOUSE OFFICE BUILDING
WASHINGTON, DC 20515–6143
MAJORITY (202) 225–5051
MINORITY (202) 225–5074
https://oversight.house.gov

MEMORANDUM

November 16, 2021

To: Members of the Committee on Oversight and Reform

Fr: Majority Committee Staff

Re: Supplemental Memo on Committee's Investigation into Ransomware

I. INTRODUCTION

Ransomware is malicious software used by cybercriminals to encrypt victims' computer systems, seize data, and extort the victims for payment in exchange for decryption or return of data.[1] In June 2021, the Committee launched an investigation into ransomware attacks and U.S. companies' payments of ransom to cybercriminals. As part of this investigation, the Committee sent letters to companies that faced ransomware attacks in the past year and paid multi-million-dollar ransoms to cybercriminal groups, including the following:

- In March 2021, **CNA Financial Corporation** (CNA), one of the country's largest insurance companies, reportedly paid a ransom of $40 million in Bitcoin after it suffered a ransomware attack from a cybercriminal group called Phoenix.[2]

- In May 2021, **Colonial Pipeline Company** (Colonial), operators of the pipeline that provides nearly half of the East Coast's fuel supply, paid DarkSide, a ransomware gang believed to operate out of Russia, a ransom of $4.4 million in Bitcoin.[3]

- In June 2021, **JBS Foods USA** (JBS), whose plants process approximately one-fifth of the United States' meat supply, paid a ransom of $11 million in Bitcoin after it suffered a ransomware attack, which the Federal Bureau of Investigation

---

[1] Cybersecurity and Infrastructure Security Agency, *Stop Ransomware: Resources* (online at www.cisa.gov/stopransomware/resources) (accessed Oct. 27, 2021).

[2] House Committee on Oversight and Reform, *Press Release: Chairwoman Maloney Presses Private Companies to Prove Details on Ransomware Payments to Cybercriminals* (June 3, 2021) (online at https://oversight.house.gov/news/press-releases/chairwoman-maloney-presses-private-companies-to-provide-details-on-ransomware).

[3] *Id.*

(FBI) attributed to the criminal ransomware gang REvil (also known as Sodinokibi).[4]

The Committee's investigation into these three ransomware attacks has provided new insights into how ransomware attacks unfold, which may aid the development of legislative and policy responses to counter the threat of ransomware. In particular, the Committee examined how attackers infect companies' systems, how cybercriminals convince companies to pay millions of dollars for uncertain decryption tools and data return, and how companies attempt to restore compromised systems after the ransom has been paid.[5] Observations include:

1. **Small lapses led to major breaches.** Ransomware attackers took advantage of relatively minor security lapses, such as a single user account controlled by a weak password, to launch enormously costly attacks. Even large organizations with seemingly robust security systems fell victim to simple initial attacks, highlighting the need to increase security education and take other security measures prior to an attack.

2. **Some companies lacked clear initial points of contact with the federal government.** Depending on their industry, companies were confronted with a patchwork of federal agencies to engage regarding the attacks they faced. For example, two companies' initial requests for assistance were forwarded around to different FBI offices and personnel before reaching the correct team. Companies also received different responses on which agencies could answer questions as to whether the attackers were sanctioned entities. These examples highlight the importance of clearly established federal points of contact.

3. **Companies faced pressure to quickly pay the ransom.** Given the uncertainty over how quickly systems could be restored using backups and whether any sensitive data was stolen, the companies appeared to have strong incentives to quickly pay the ransom. This pressure was compounded by attackers' assurances that payment of the ransom would resolve the situation and avoid negative publicity for the company. For instance, after the initial hack of JBS, REvil told the company, "We can unblock your data and keep everything secret. All we need is a ransom."[6] Further examination is needed of the factors encouraging ransom payments, including the role of cyber insurance and the costs companies can face even after paying a ransom, especially when the cybercriminals fail to deliver on their promises.

---

[4] House Committee on Oversight and Reform, *Press Release: Chairwoman Maloney Expands Committee's Ransomware Investigation to JBS Foods* (June 11, 2021) (online at https://oversight house.gov/news/press-releases/chairwoman-maloney-expands-committee-s-ransomware-investigation-to-jbs-foods).

[5] Majority staff consulted with federal law enforcement to ensure that the information obtained by the Committee and included in this memorandum and the enclosed documents would not interfere with any law enforcement investigations or prosecutions. Neither the Federal Bureau of Investigations nor the Department of Justice raised any concerns regarding this information.

[6] Communications between JBS Foods USA and Attackers (May 31, 2021).

II. THE INTRUSION

In all three attacks, the cybercriminals appear to have accessed and infected the companies' computer systems due to small failures in their security systems. Colonial's chief executive officer (CEO) has previously explained that the attack on the company's systems started with a single stolen password linked to an old user profile.[7] In the case of JBS, the attackers gained access to an old network administrator account that had not been deactivated and was protected only by a weak password.[8] CNA's attackers convinced a single employee to accept a fake web browser update from a commercial website.[9]

For CNA and JBS, the breaches were not immediately detected.[10] The attackers' presence on CNA's network went undetected for over two weeks before the ransomware was activated.[11]

Once the ransomware was deployed by the attackers, it quickly crippled companies' IT systems. On May 7, 2021, after a Colonial employee discovered a ransom note,[12] Colonial shut down its entire pipeline operations out of concern that the malicious software might allow the attackers to gain physical control of the pipeline.[13] It remained offline for five days before gradually reopening.[14] The attack on JBS caused the company's plants to temporarily shut

---

[7] *One Password Allowed Hackers to Disrupt Colonial Pipeline, CEO Tells Senators*, Reuters (June 8, 2021) (online at www.reuters.com/business/colonial-pipeline-ceo-tells-senate-cyber-defenses-were-compromised-ahead-hack-2021-06-08/); House Committee on Homeland Security, Written Testimony of Charles Carmakal, Senior Vice President and Chief Technology Officer, FireEye-Mandiant, *Hearing on Cyber Threats in the Pipeline: Using Lessons from the Colonial Ransomware Attack to Defend Critical Infrastructure* (June 9, 2021) (online at https://homeland.house.gov/imo/media/doc/2021-06-09-HRG-Testimony%20Carmakal.pdf).

[8] Briefing by JBS Foods USA for Staff, House Committee on Oversight and Reform (July 21, 2021).

[9] Letter from Norton Rose Fulbright, on behalf of CNA Financial Corporation, to Consumer Protection Bureau, Office of the Attorney General of New Hampshire (July 8, 2021) (online at https://s3.documentcloud.org/documents/21014668/cna-financial-bc-legal-notice-sec-incident.pdf).

[10] *Id.*; *JBS Hackers Took Data from Australia and Brazil, Researcher Says*, Bloomberg (June 8, 2021) (online at www.bloomberg.com/news/articles/2021-06-08/jbs-hackers-took-data-from-australia-and-brazil-researcher-says).

[11] Letter from Norton Rose Fulbright, on behalf of CNA Financial Corporation, to Consumer Protection Bureau, Office of the Attorney General of New Hampshire (July 8, 2021) (online at https://s3.documentcloud.org/documents/21014668/cna-financial-bc-legal-notice-sec-incident.pdf).

[12] Ransom Note Left on Colonial Pipeline Company's Computer Systems (May 7, 2021) (Exhibit B).

[13] *Colonial Pipeline Was Shut Down with Worst-Case Scenario in Mind, Executives Say*, Washington Post (June 9, 2021) (online at www.washingtonpost.com/business/2021/06/09/colonial-pipeline-mandiant-house-hearing/).

[14] Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021); *Colonial Pipeline Restarts After Hack, but Supply Chain Won't Return to Normal for a Few Days*, CNBC (May 12, 2021) (online at www.cnbc.com/2021/05/12/colonial-pipeline-restarts-after-hack-but-supply-chain-wont-return-to-normal-for-a-few-days.html).

down.[15] In the case of CNA, cybercriminals encrypted its computer systems and stole substantial amounts of company data, including personal information.[16]

Given the widespread impact to company networks, company executives coordinated their response using personal email accounts and text messages. For example, the Committee obtained an email from a senior JBS employee notifying an FBI field office of the ransomware attack and requesting assistance, which was sent from the JBS employee's personal account.[17]

The Committee's investigation also underscored the logistical challenges of the companies' response to these attacks, which differed in part based on the company's industry. Each company provided notice to a variety of different federal agencies, including federal law enforcement.[18] For example, Colonial was in contact with at least seven federal agencies or offices.[19] CNA was initially referred to one FBI field office before a different field office was designated as the primary point of contact.[20] When a senior JBS official first emailed an FBI field office, the agent they emailed was not the correct point of contact, so their inquiry was passed on to different case agents at the same field office, leading to a several-hour delay between the JBS official's initial email and the FBI's first substantive email response.[21] In one instance, a company was referred to the Treasury Department for questions regarding sanctions, while another company was provided a substantive answer on this topic by the FBI.[22] These

[15] *JBS Paid $11 Million to Resolve Ransomware Attack*, Wall Street Journal (June 9, 2021) (online at www.wsj.com/articles/jbs-paid-11-million-to-resolve-ransomware-attack-11623280781).

[16] CNA Financial Corporation, *Formal Notice of Cybersecurity Incident* (July 9, 2021) (online at https://s3.documentcloud.org/documents/20986305/cna-legal-notice-070921.pdf); *Insurance Giant CNA Reports Data Breach After Ransomware Attack*, Bleeping Computer (July 9, 2021) (online at www.bleepingcomputer.com/news/security/insurance-giant-cna-reports-data-breach-after-ransomware-attack/).

[17] Email from [Name Redacted], JBS Foods USA, to [Name Redacted], Federal Bureau of Investigation (May 30, 2021) (Exhibit D); Email from [Name Redacted], Federal Bureau of Investigation, to [Name Redacted], JBS Foods USA (May 31, 2021) (Exhibit E).

[18] Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021); Briefing by CNA Financial Corporation for Staff, Committee on Oversight and Reform (July 13, 2021); Briefing by JBS Foods USA for Staff, Committee on Oversight and Reform (July 21, 2021).

[19] Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021); Senate Committee on Homeland Security and Governmental Affairs, Written Testimony of Joseph Blount, President and Chief Executive Officer, Colonial Pipeline Company, *Hearing on Threats to Critical Infrastructure: Examining the Colonial Pipeline Cyber Attack* (June 8, 2021) (online at www hsgac.senate.gov/imo/media/doc/Testimony-Blount-2021-06-08.pdf).

[20] Briefing by CNA Financial Corporation for Staff, House Committee on Oversight and Reform (July 13, 2021).

[21] Email from [Name Redacted], JBS Foods USA, to Federal Bureau of Investigation (May 30, 2021) (Exhibit D); Email from Federal Bureau of Investigation to [Name Redacted], JBS Foods (May 31, 2021) (Exhibit E).

[22] Email from [Name Redacted], Federal Bureau of Investigation, to [Name Redacted], JBS Foods USA (June 1, 2021); Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021).

logistical hurdles underscore the need for clearly established federal points of contact in response to ransomware attacks.

III. THE NEGOTIATION: PRESSURE TO QUICKLY PAY RANSOM

Following the discoveries of the intrusions, all three companies faced immediate and repeated pressure from the attackers to quickly pay the ransom. Although tactics differed, attackers pressed the companies to make payment quickly by: (1) increasing ransom demands, (2) threatening to release large caches of data, and (3) setting arbitrary time limits.

After the cybercriminal group REvil deployed its ransomware on JBS's system, they sent JBS a message demanding a payment of $22.5 million. The ransom message warned that the price would double if payment was not made in a certain period.[23] The attackers also warned, "We have all your network data," and, "if you do not reply us within 3 days it will be posted on our news-site." REvil encouraged JBS to "Think about the financial damage to your stock price from this publication" and promised a "good discount in case of quick payment." They also assured JBS, "We can unblock your data and keep everything secret. All we need is a ransom."[24]

JBS explained to the Committee that in addition to the cost of rebuilding its systems from backups if it did not pay the ransom, the company faced other pressing concerns and potential costs, including obligations to customers and employees, as well as the need to process meat carcasses in its facilities, potentially totaling tens of millions of carcasses per day.[25] Eventually, JBS and the attackers agreed on an $11 million ransom.

Colonial was initially informed that the ransom was $4.8 million but that the price would increase to $9.6 million after a set amount of time, as marked by a timer in a corner of the screen.[26]

During the attack on CNA, the attackers informed the company that the cost for decryption was "999 bitcoins," or the equivalent of roughly $55 million at the time. The attackers subsequently raised the price without warning, stating, "Wasting time. The cost went up, 1099 BTC." The attackers added, "CNA data we have is important. It will hit hard if leaked." The hackers also assured CNA that they would not publish anything about this incident or talk to the press if the company paid the ransom.[27]

Attackers also refused to provide clarity on what data had been stolen from the companies as part of the attack. During the attack on JBS, after initially agreeing to provide

---

[23] Ransom Note Left on JBS Foods USA Computer Systems (May 31, 2021) (Exhibit C); Communications between JBS Foods USA and Attackers (May 31, 2021).

[24] Communications between JBS Foods USA and Attackers (May 31, 2021).

[25] Briefing by JBS Foods USA for Staff, Committee on Oversight and Reform (July 21, 2021).

[26] Ransom Note Left on Colonial Pipeline Company Computer Systems (May 7, 2021) (Exhibit B).

[27] Communications between CNA Financial Corporation and Attackers (Mar. 23, 2021).

examples of data taken from the company's network, the cybercriminals reversed course, stating, "After analyzing the available information, my boss came to the conclusion that the transfer of files will take place only after payment."[28]

Despite launching cyberattacks on the companies, the attackers attempted to cast themselves as business partners with, or even consultants to, the companies. REvil told JBS, "don't panic! We are in business, not in war," and offered the company a host of supposed benefits along with the decryption tool, stating, "in this case, you also get a security report, a complete tree of compromised data files, permanently deleting downloaded data, [and] support with tips on unlocking and protecting."[29] The REvil attackers even provided recommendations of exchanges where the company could buy cryptocurrency, highlighting that one exchange had "no need for verification."[30] In the case of Colonial, DarkSide warned there was one data recovery company they refused to work with but offered to recommend others.[31]

During the attack on Colonial, DarkSide stated: "We have helped more than 100 companies. And we will help you after payment."[32] In the case of JBS, REvil also disclaimed any interest in the security or economic effects caused by the attack on the company or the shutdown of its food processing plants, stating: "Its just a business. We absolutely do not care about you or your deals, except getting benefits."[33]

Although the FBI has a general policy discouraging payments to ransomware attackers,[34] JBS and Colonial ultimately made the decision to pay, as CNA reportedly did as well. Colonial's CEO has also publicly stated that he judged his company's payment to be "the right thing to do for the country."[35] JBS told Committee staff that they did not inform the government of their specific plans to pay the ransom.[36] JBS also indicated federal officials were pleased that the company was able to quickly restore capacity to support the nation's food supply.[37]

---

[28] Communications between JBS Foods USA and Attackers (May 31, 2021).

[29] Communications between JBS Foods USA and Attackers (May 31, 2021).

[30] Ransom Note Left on JBS Foods USA Computer Systems (May 30, 2021) (Exhibit C).

[31] Ransom Note Left on Colonial Pipeline Company's Computer Systems (May 7, 2021) (Exhibit B).

[32] Communications between Colonial Pipeline Company and Attackers (May 7, 2021).

[33] Ransom Note Left on JBS Foods USA Computer Systems (May 30, 2021) (Exhibit C).

[34] Federal Bureau of Investigation, *Ransomware* (online at www fbi.gov/scams-and-safety/common-scams-and-crimes/ransomware) (accessed Nov. 10, 2021).

[35] *Colonial Pipeline CEO Tells Why He Paid Hackers a $4.4 Million Ransom*, Wall Street Journal (May 19, 2021) (online at www.wsj.com/articles/colonial-pipeline-ceo-tells-why-he-paid-hackers-a-4-4-million-ransom-11621435636).

[36] Briefing by JBS Foods USA for Staff, House Committee on Oversight and Reform (July 21, 2021).

[37] *Id.*

The companies made these decisions despite having at least some system backups that were not affected by the attacks.[38] JBS, which paid one of the largest known cyber ransoms in history, later revealed, "At the time of payment, the vast majority of the company's facilities were operational," and explained that it paid the ransom to "mitigate any unforeseen issues related to the attack and ensure no data was exfiltrated."[39] Two of the three companies, Colonial and CNA, also had cyber insurance policies.[40] Colonial has confirmed to the Committee that its cybersecurity insurance policy covered the cost of the ransom.[41]

IV. THE AFTERMATH

During the attacks, the attackers also provided certain assurances that they would follow through with promises to provide a decryption key and delete their copies of the stolen data if a ransom was paid. Attackers told CNA they would know if stolen data had been deleted because, "We gonna tell you 'the data was deleted,'" later adding, "It is in our interest to do as agreed."[42] CNA later recovered the data with the assistance of consultants by locating a repository used by the attackers.[43] In the case of JBS, the REvil attackers never delivered on their promise to provide the company with proof that they had destroyed all copies of the data they stole from JBS.[44]

While the decryption keys provided by the cybercriminals appear to have worked, it is unclear whether using the decryption keys was the most effective option. Colonial informed the Committee that while it used the decryption key to decrypt some individual files, it did not use the decryption key more broadly for two reasons. First, the process of using the decryption key presented a risk of deleting legitimate files. Second, Colonial determined that using its back-up tapes was the better approach to bringing its systems back online.[45] According to press reports, Colonial relied on its backup tapes because the tool provided by DarkSide was too slow to be

---

[38] *Id.*; Briefing by CNA Financial Corporation for Staff, House Committee on Oversight and Reform (July 13, 2021); Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021).

[39] Communications between JBS Foods USA and Attackers (May 31, 2021); *Beef Supplier JBS Paid Ransomware Hackers $11 Million*, NBC News (June 9, 2021) (online at www.nbcnews.com/tech/security/meat-supplier-jbs-paid-ransomware-hackers-11-million-n1270271).

[40] *Colonial Pipeline Has Cyber Insurance Policy—Sources*, Reuters (May 13, 2021) (online at www reuters.com/business/energy/colonial-pipeline-has-cyber-insurance-policy-sources-2021-05-13/); *CNA Says Insurance Unlikely to Cover Cyberattack in Full*, Law360 (Nov. 2, 2021) (online at www.law360.com/insurance-authority/articles/1436982).

[41] Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021).

[42] Communications between Colonial Pipeline Company and Attackers (Mar 25, 2021).

[43] Briefing by CNA Financial Corporation for Staff, House Committee on Oversight and Reform (July 13, 2021).

[44] Communications between JBS Foods USA and Attackers (June 10, 2021).

[45] Letter from Drew Lohoff, Director, Government Affairs, Colonial Pipeline Company, to Chairwoman Carolyn B. Maloney, House Committee on Oversight and Reform (June 17, 2021).

useful.[46] In the case of CNA, months after regaining access to its files, the company was still in the process of notifying customers and employees of the data breach, as well as providing them with credit monitoring and fraud prevention services in light of the compromised personal information.[47]

[46] *Colonial Pipeline Paid Hackers Nearly $5 Million in Ransom*, Bloomberg (May 13, 2021) (online at www.bloomberg.com/news/articles/2021-05-13/colonial-pipeline-paid-hackers-nearly-5-million-in-ransom).

[47] Letter from Norton Rose Fulbright, on behalf of CNA Financial Corporation, to Consumer Protection Bureau, Office of the Attorney General of New Hampshire (July 8, 2021) (online at https://s3.documentcloud.org/documents/21014668/cna-financial-bc-legal-notice-sec-incident.pdf).

List of Exhibits

Exhibit A: Ransom Note Left on CNA Financial Corporation's Computer Systems (March 21, 2021)

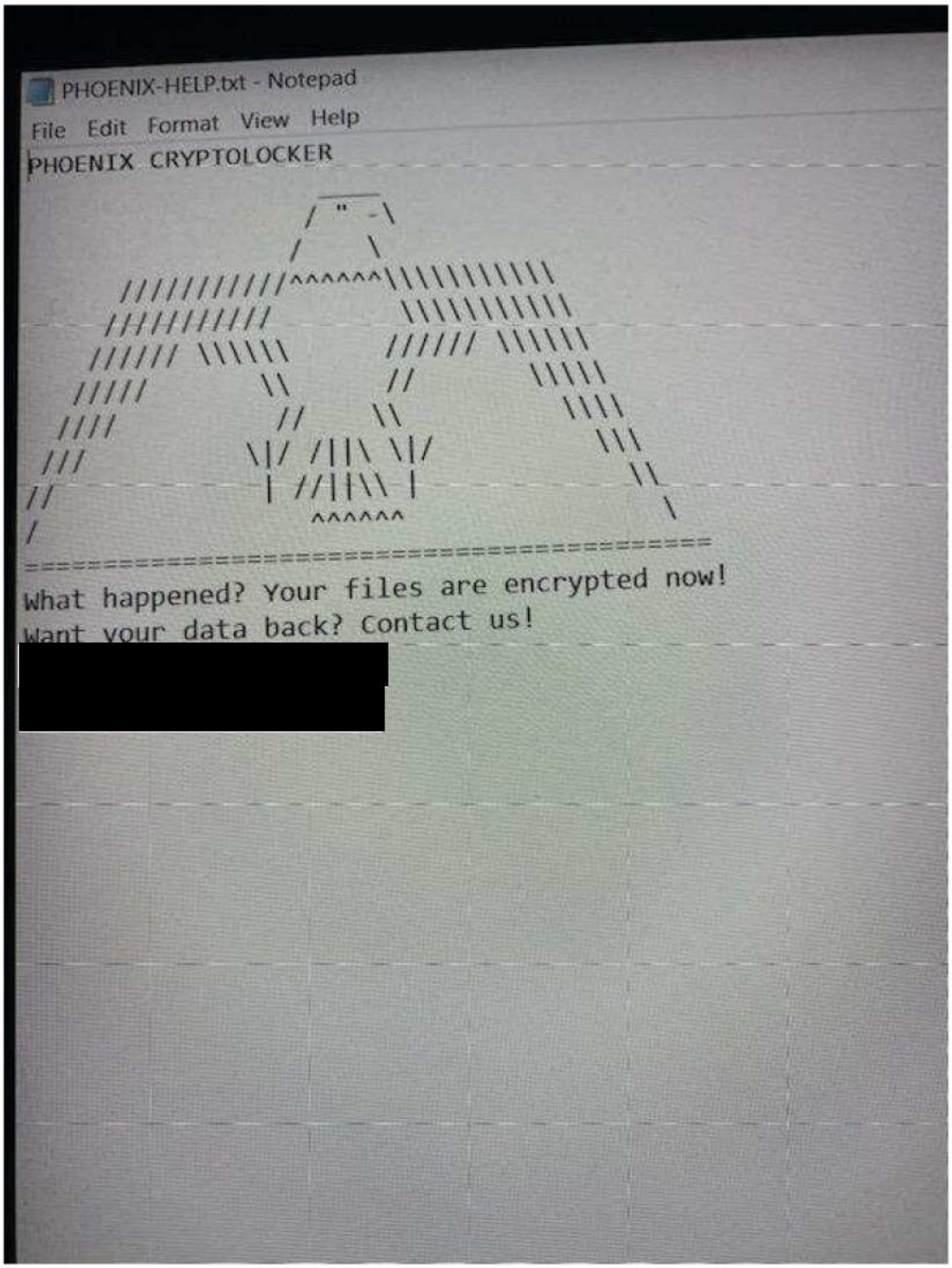

PHOENIX-HELP.txt - Notepad
File Edit Format View Help
PHOENIX CRYPTOLOCKER
What happened? Your files are encrypted now!
Want your data back? Contact us!
[redacted]

Exhibit B: Colonial Pipeline Company Computer Systems (May 7, 2021)

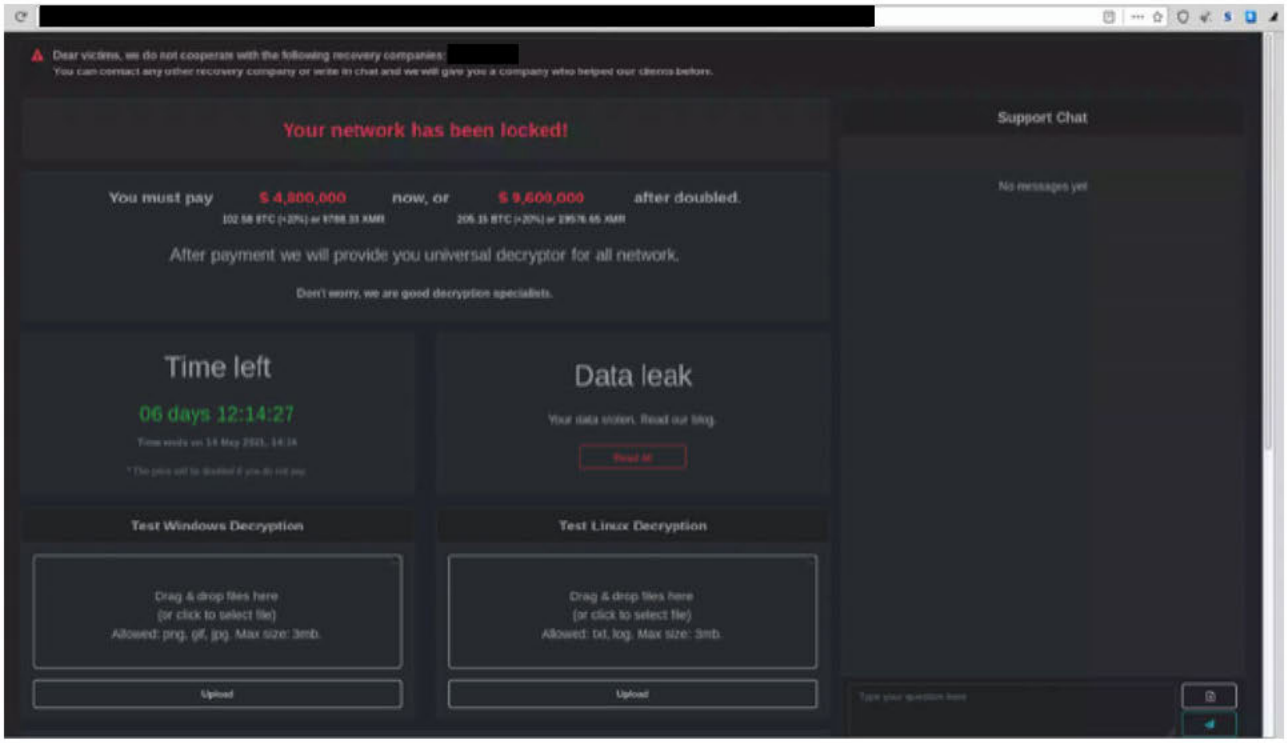

[redacted]
Dear victims, we do not cooperate with the following recovery companies: [redacted]
You can contact any other recovery company or write in chat and we will give you a company who helped our clients before.
Your network has been locked!
You must pay $ 4,800,000 now, or $ 9,600,000 after doubled.
102.58 BTC (+20%) or 9788.33 XMR
205.15 BTC (+20%) or 19576.65 XMR
After payment we will provide you universal decryptor for all network.
Don't worry, we are good decryption specialists.
Time left
06 days 12:14:27
Time ends on 14 May 2021, 14:14
* The price will be doubled if you do not pay
Data leak
Your data stolen. Read our blog.
Read it!
Test Windows Decryption
Drag & drop files here
(or click to select file)
Allowed: png, gif, jpg. Max size: 3mb.
Upload
Test Linux Decryption
Drag & drop files here
(or click to select file)
Allowed: txt, log. Max size: 3mb.
Upload
Support Chat
No messages yet
Type your question here

Exhibit C: Ransom Notes Left on JBS Foods USA Computer Systems (May 30, 2021)

---=== Welcome. Again. ===---

[+] Whats Happen? [+]

Your files are encrypted, and currently unavailable. You can check it:
all files on your system has extension 6vax1.
By the way, everything is possible to recover (restore), but you need to
follow our instructions. Otherwise, you cant return your data (NEVER).

[+] What guarantees? [+]

Its just a business. We absolutely do not care about you and your deals,
except getting benefits. If we do not do our work and liabilities -
nobody will not cooperate with us. Its not in our interests.
To check the ability of returning files, You should go to our website.
There you can decrypt one file for free. That is our guarantee.
If you will not cooperate with our service - for us, its does not matter.
But you will lose your time and data, cause just we have the private key.
In practise - time is much more valuable than money.

[+] How to get access on website? [+]

You have two ways:

1) [Recommended] Using a TOR browser!
  a) Download and install TOR browser from this site:
https://torproject.org/
  b) Open our website:
[redacted]

2) If TOR blocked in your country, try to use VPN! But you can use our
secondary website. For this:
  a) Open your any browser (Chrome, Firefox, Opera, IE, Edge)
  b) Open our secondary website: [redacted]

Warning: secondary website can be blocked, thats why first variant much
better and more available.

When you open our website, put the following data in the input form:
Key:

[redacted]

!!! DANGER !!!
DONT try to change files by yourself, DONT use any third party software for restoring your data or antivirus solutions - its may entail damge of the private key and, as result, The Loss all data.
!!! !!! !!!
ONE MORE TIME: Its in your interests to get your files back. From our side, we (the best specialists) make everything for restoring, but please should not interfere.
!!! !!! !!!

Your network has been infected!

Your documents, photos, databases and other important files **encrypted**

To decrypt your files you need to buy our special software - General-Decryptor

Follow the instructions below. But remember that you do not have much time

General-Decryptor price

the price is for all PCs of your infected network

You have 4 days, 16:54:38

* If you do not pay on time,the price will be double
* Time ends on Jun 4, 14:39:24

Current price 84736.125 XMR
≈ 22,500,000 USD

After time ends 169472.25 XMR
≈ 45,000,000 USD

Monero address: [redacted]

* XMR will be recalculated in 4 hours with an actual rate

INSTRUCTIONS | CHAT SUPPORT | ABOUT US

How to decrypt files?

You will not be able to decrypt the files yourself. If you try, you will lose your files forever.

Buy XMR (no need for verification)

[redacted]

To decrypt your files you need to buy our special software General-Decryptor.

* If you need guarantees, use trial decryption below

How to buy General-Decryptor?

1. Buy the required amount of XMR (Monero): **84736.125 XMR**

If you have problems with buying XMR, you can buy BTC (Bitcoin) and exchange it for XMR. See «Exchange BTC for XMR» on the page.

2. Send **84736.125 XMR** to the following Monero address:

[redacted]

* This receiving address was created for you, to identify your transaction

3. Wait for **10** confirmations by blockchain

4. Reload current page after, and get a link to download General-Decryptor

Trial decryption

Upload your image file for trial decryption to make sure the General-Decryptor works.

* This file should be an encrypted image. Example:

- your-image.jpg.g5mr45
- your-image.png.g5mr45
- your-image.gif.g5mr45

* This file should be an encrypted image

Browse...

Buy XMR with Bank

[redacted]

Buy XMR locally with cash or online

[redacted]

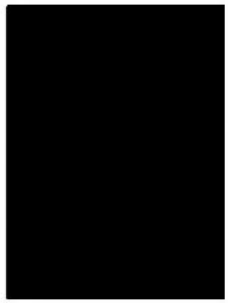
Buy XMR from India or South Korea

[redacted]

Buy Bitcoin and trade for XMR

[redacted]

Other services where you can buy BTC, needed to exchange for XMR:



Exchange BTC for XMR

Exhibit D: Email from [Name Redacted], JBS Foods USA, to [Name Redacted], Federal Bureau of Investigation (May 30, 2021)

On May 31, 2021, at 11:23 AM, [redacted]@fbi.gov> wrote:

Hello [redacted]

My apologies for the delay in replying. I am not the case Agent for Sodinokibi. The lead case Agents for Sodinokibi are SA's [redacted](copied). Please feel free to go direct with either of them.

Special Agent [redacted]
Federal Bureau of Investigation
[redacted]

From: [redacted]@gmail.com>
Sent: Sunday, May 30, 2021 9:41 PM
To: [redacted]@fbi.gov>
Subject: [EXTERNAL EMAIL] - Sodinokibi

[redacted]

My name is [redacted] and I am General Counsel for JBS USA Food Company, a subsidiary of JBS SA, the world's largest food company.

Today we suffered a cyber attack and ransom demand by Sodinokibi. I understand you are the lead Agent handling issues with this threat actor.

If you could please give me a call on my cell as soon as possible (number below), I would very much appreciate it.

Thank you,
[redacted]
General Counsel
[redacted]

Exhibit E: Email from [Name Redacted], Federal Bureau of Investigation, to [Name Redacted], JBS Foods USA (May 31, 2021)

On May 31, 2021, at 5:41 PM, [redacted]@fbi.gov> wrote:

Good evening.
The FBI [redacted] would like to provide JBS USA Food management a [redacted] tonight via [redacted]. Is this something we can schedule tonight? If so, please let me know a time tonight that works for you and copy those individuals on your response back to me. [redacted]

[redacted]

[redacted]

Special Agent

Federal Bureau of Investigation | [redacted]

National Security Cyber Squad

[redacted]

From: [redacted]@gmail.com>
Sent: Monday, May 31, 2021 1:00 PM
To: [redacted]@fbi.gov>
Cc: [redacted]@fbi.gov>; [redacted]@fbi.gov>; [redacted]@jbssa.com>
Subject: IMPORTANT: [EXTERNAL EMAIL] - Sodinokibi

Thank you, [redacted]

[redacted]

My name is [redacted] and I am General Counsel for JBS USA Food Company ("JBS"). Also on this email is our Chief Legal Officer [redacted].

As mentioned below, JBS is a wholly-owned subsidiary of JBS SA, the world's largest meat processing company and second-largest food company.

Early yesterday morning, we suffered a cyber attack by Sodinokibi, who has demanded the equivalent of USD$22.5M in cryptocurrency. Their attack has completely impacted our beef, lamb, pork, and chicken operations in all of North America and Australia. As of right now, we cannot operate any of our plants. This has the potential of GREATLY disrupting the food supply chain in these geographies.

If one of you could please contact me at your earliest convenience, I would really appreciate it.

Thank you,
[redacted]
General Counsel
[redacted]