Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

1 September 2021

PIN Number
20210901-001

Please contact the FBI with any questions related to this Private Industry Notification at either your local **Cyber Task Force** or **FBI CyWatch**.

Local Field Offices:
www.fbi.gov/contact-us/field-offices

E-mail:
cywatch@fbi.gov

Phone:
1-855-292-3937

Cyber Criminal Actors Targeting the Food and Agriculture Sector with Ransomware Attacks

Summary

Ransomware attacks targeting the Food and Agriculture sector disrupt operations, cause financial loss, and negatively impact the food supply chain. Ransomware may impact businesses across the sector, from small farms to large producers, processors and manufacturers, and markets and restaurants. Cyber criminal threat actors exploit network vulnerabilities to exfiltrate data and encrypt systems in a sector that is increasingly reliant on smart technologies, industrial control systems, and internet-based automation systems.

Food and agriculture businesses victimized by ransomware suffer significant financial loss resulting from ransom payments, loss of productivity, and remediation costs. Companies may also experience the loss of proprietary information and personally identifiable information (PII) and may suffer reputational damage resulting from a ransomware attack.

Private Industry Notification
FEDERAL BUREAU OF INVESTIGATION, CYBER DIVISION

Threat Overview

The Food and Agriculture sector is among the critical infrastructure sectors increasingly targeted by cyber attacks. As the sector moves to adopt more smart technologies and internet of things (IoT) processes the attack surface increases. Larger businesses are targeted based on their perceived ability to pay higher ransom demands, while smaller entities may be seen as soft targets, particularly those in the earlier stages of digitizing their processes, according to a private industry report.

In a ransomware attack, victims' files are encrypted and made unavailable, and the attacker demands a payment for the decryption tool and key. As of 2019, sensitive data files are commonly exfiltrated prior to encryption, and the attacker demands a payment not to publish the sensitive data on a "name-and-shame" website. This double extortion potentially gives the attacker more leverage to ensure payment, based on the potential damage caused by a significant data breach of sensitive information. Threat actors may apply additional coercive tactics such as convincing media organizations to write stories on victim security incidents, harassing employees by phone, notifying business partners of data theft, and conducting distributed denial of service attacks to further disrupt operations. According to a private industry report, cyber actors may gradually broaden their attack from just information technology (IT) and business processes to also include the operational technology (OT) assets, which monitor and control physical processes, impacting industrial production regardless of whether the malware was deployed in IT or OT systems.

The impact of ransomware attacks continues to grow. From 2019 to 2020, the average ransom demand doubled and the average cyber insurance payout increased by 65 percent from 2019 to 2020. The highest observed ransom demand in 2020 was $23 million USD, according to a private industry report. According to the 2020 IC3 Report, IC3 received 2,474 complaints identified as ransomware with adjusted losses of over $29.1 million across all sectors. Separate studies have shown 50-80 percent of victims that paid the ransom experienced a repeat ransomware attack by either the same or different actors. Although cyber criminals use a variety of techniques to infect victims with ransomware, the most common means of infection are email phishing campaigns, Remote Desktop Protocol (RDP) vulnerabilities, and software vulnerabilities.

Examples of ransomware attacks impacting food and agriculture sector businesses include the following:

- In July 2021, a US bakery company lost access to their server, files, and applications, halting their production, shipping, and receiving as a result of Sodinokibi/REvil ransomware which was deployed through software used by an IT support managed service provider (MSP). The bakery company was shut down for approximately one week, delaying customer orders and damaging the company's reputation.
- In May 2021, cyber actors using a variant of the Sodinokibi/REvil ransomware compromised computer networks in the US and overseas locations of a global meat processing company, which resulted in the possible exfiltration of company data and the shutdown of some US-based plants

for several days. The temporary shutdown reduced the number of cattle and hogs slaughtered, causing a shortage in the US meat supply and driving wholesale meat prices up as much as 25 percent, according to open source reports.

- In March 2021, a US beverage company suffered a ransomware attack that caused significant disruption to its business operations, including its operations, production, and shipping. The company took its systems offline to prevent the further spread of malware, directly impacting employees who were unable to access specific systems, according to open source reports.
- In January 2021, a ransomware attack against an identified US farm resulted in losses of approximately $9 million due to the temporary shutdown of their farming operations. The unidentified threat actor was able to target their internal servers by gaining administrator level access through compromised credentials.
- In November 2020, a US-based international food and agriculture business reported it was unable to access multiple computer systems tied to their network due to a ransomware attack conducted by OnePercent Group threat actors using a phishing email with a malicious zip file attachment. The cybercriminals downloaded several terabytes of data through their identified cloud service provider prior to the encryption of hundreds of folders. The company's administrative systems were impacted. The company did not pay the $40 million ransom and was able to successfully restore their systems from backups.

Recommended Mitigations

Cyber criminal threat actors will continue to exploit network system vulnerabilities within the food and agriculture sector. The following steps can be implemented to mitigate the threat and protect against ransomware attacks:

- Regularly back up data, air gap, and password protect backup copies offline. Ensure copies of critical data are not accessible for modification or deletion from the system where the data resides.
- Implement network segmentation.
- Implement a recovery plan to maintain and retain multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication with strong pass phrases where possible.
- Use strong passwords and regularly change passwords to network systems and accounts, implementing the shortest acceptable timeframe for password changes. Avoid reusing passwords for multiple accounts.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.

- Require administrator credentials to install software.
- Audit user accounts with administrative privileges and configure access controls with least privilege in mind.
- Install and regularly update anti-virus and anti-malware software on all hosts.
- Only use secure networks and avoid using public Wi-Fi networks. Consider installing and using a VPN.
- Consider adding an email banner to messages coming from outside your organizations.
- Disable hyperlinks in received emails.
- Focus on cyber security awareness and training. Regularly provide users with training on information security principles and techniques as well as overall emerging cybersecurity risks and vulnerabilities (i.e. ransomware and phishing scams).

For additional information on ransomware, see also:

- FLASH-CU-000149-MW "Indicators of Compromise Associated with OnePercent Group Ransomware" (TLP: WHITE)
- FLASH-CU-000145-MW "Indicators Associated with Avaddon Ransomware" (TLP:GREEN)
- FLASH-CP-000147-MW-Conti – "Conti Ransomware Attacks Impact Healthcare and First Responder Networks" (TLP:WHITE)
- JCA-AA21-131A-Darkside – "Darkside Ransomware: Best Practices for Preventing Business Disruption from Ransomware Attacks" (TLP:WHITE)
- FLASH-MU-000146-MW-DARKSIDE – "Indicators of Compromise Associated with Darkside Ransomware" (TLP:GREEN)
- FLASH-MU-000144-MW-Nefilim – "Indicators of Compromise Associate with Nefilim Ransomware" (TLP:GREEN)
- FLASH-CU-000143-MW-Mamba-Ransomware – "Mamba Ransomware Weaponizing DiskCryptor" (TLP:WHITE)
- FLASH-CP-000142-MW-PYSA-Ransomware – "Increase in PYSA Ransomware Targeting Education Institutions" (TLP:WHITE)

Information Requested

The FBI is seeking any information that can be shared, to include boundary logs showing communication to and from foreign IP addresses, Bitcoin wallet information, the decryptor file, and/or a benign sample of an encrypted file. The FBI does not encourage paying ransoms. Payment does not guarantee files will be recovered. It may also embolden adversaries to target additional organizations, encourage other criminal actors to engage in the distribution of ransomware, and/or fund illicit activities. However, the FBI understands that when victims are faced with an inability to function, all options are evaluated to protect shareholders, employees and customers. Regardless of whether you or your organization have decided to pay the ransom, the FBI urges you to promptly

report ransomware incidents to your local field office or the FBI's 24/7 Cyber Watch (CyWatch). Doing so provides the FBI with critical information needed to prevent future attacks by identifying and tracking ransomware attackers and holding them accountable under U.S. law.

Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to https://www.stopransomware.gov as well as the CISA-Multi-State Information Sharing and Analysis Center (MS-ISAC) Joint Ransomware Guide. Stopransomware.gov is the U.S. Government's new, official one-stop location for resources to tackle ransomware more effectively.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to either a local FBI field office at www.fbi.gov/contact-us/field-offices or to the FBI's 24/7 Cyber Watch at (855) 292-3937 or CyWatch@fbi.gov. Indicate the type of activity, date, time, location and, if known, the number of people involved and type of equipment used. Reports should include the name of the company or organization submitting the complaint and a point of contact. Direct press inquiries to the FBI National Press Office at (202) 324-3691 or npo@fbi.gov.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, **TLP:WHITE** information may be distributed without restriction. For comments or questions related to the content or dissemination of this product, contact the FBI Cyber Watch.

Your Feedback Regarding this Product is Critical.

Please take a few minutes to send us your feedback about this product. Feedback that is specific to your experience with FBI written products enables us to make continuous improvements. We read each submission carefully and value all comments. Submit feedback online here: https://www.ic3.gov/PIFSurvey