Private Industry Notification

FEDERAL BUREAU OF INVESTIGATION • CYBER DIVISION

20 April 2022

PIN Number

20220420-001

Please contact the FBI with any questions related to this Private Industry Notification via your local FBI Cyber Squad.

www.fbi.gov/contact-us/field-offices

Ransomware Attacks on Agricultural Cooperatives Potentially Timed to Critical Seasons

Summary

The Federal Bureau of Investigation (FBI) is informing Food and Agriculture (FA) sector partners that ransomware actors may be more likely to attack agricultural cooperatives during critical planting and harvest seasons, disrupting operations, causing financial loss, and negatively impacting the food supply chain. The FBI noted ransomware attacks during these seasons against six grain cooperatives during the fall 2021 harvest and two attacks in early 2022 that could impact the planting season by disrupting the supply of seeds and fertilizer. Cyber actors may perceive cooperatives as lucrative targets with a willingness to pay due to the time-sensitive role they play in agricultural production. Although ransomware attacks against the entire farm-to-table spectrum of the FA sector occur on a regular basis, the number of cyber attacks against agricultural cooperatives during key seasons is notable.

According to a February 2022 Joint Cybersecurity Advisory[1] authored by cybersecurity authorities in the United States, Australia, and the United Kingdom, ransomware tactics and techniques continued to evolve in 2021. Sophisticated, high-impact ransomware incidents

[1] Product ID: AA22-040A, 2021 Trends Show Increased Globalized Threat [TLP:WHITE]

against critical infrastructure organizations increased globally. The FBI, the Cybersecurity and Infrastructure Security Agency (CISA), and the National Security Agency (NSA) observed incidents involving ransomware against 14 of the 16 U.S. critical infrastructure sectors, including FA, the Defense Industrial Base, Emergency Services, Government Facilities, and Information Technology Sectors.

Threat

Since 2021, multiple agricultural cooperatives have been impacted by a variety of ransomware variants. Initial intrusion vectors included known but unpatched common vulnerabilities and exploits, as well as secondary infections from the exploitation of shared network resources or compromise of managed services. Production was impacted for some of the targeted entities, resulting in slower processing due to manual operations, while other targeted entities lost access to administrative functions such as websites and email but did not have production impacted.

A significant disruption of grain production could impact the entire food chain, since grain is not only consumed by humans but also used for animal feed. In addition, a significant disruption of grain and corn production could impact commodities trading and stocks. An attack that disrupts processing at a protein or dairy facility can quickly result in spoiled products and have cascading effects down to the farm level as animals cannot be processed.

- In March 2022, a multi-state grain company suffered a Lockbit 2.0 ransomware attack. In addition to grain processing, the company provides seed, fertilizer, and logistics services, which are critical during the spring planting season.
- In February 2022, a company providing feed milling and other agricultural services reported two instances in which an unauthorized actor gained access to some of its systems and may have attempted to initiate a ransomware attack. The attempts were detected and stopped before encryption occurred.
- Between 15 September and 6 October 2021, six grain cooperatives experienced ransomware attacks. A variety of ransomware variants were used, including Conti, BlackMatter, Suncrypt, Sodinokibi, and BlackByte. Some targeted entities had to completely halt production while others lost administrative functions.
- In July 2021, a business management software company found malicious activity on its network, which was later identified as HelloKitty/Five Hands ransomware. The threat actor demanded $30 million USD ransom. The ransomware attack on the company led to secondary ransomware infections on a number of its clients, which included several agricultural cooperatives.

Recommendations

Cyber threat actors will continue to exploit network, system, and application vulnerabilities within the FA 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 a recovery plan that includes maintaining and retaining multiple copies of sensitive or proprietary data and servers in a physically separate, segmented, secure location (i.e., hard drive, storage device, the cloud).
- Identify critical functions and develop an operations plan in the event that systems go offline. Think about ways to operate manually if it becomes necessary.
- Implement network segmentation.
- Install updates/patch operating systems, software, and firmware as soon as they are released.
- Use multifactor authentication 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 and use strong pass phrases where possible.
- Disable unused remote access/RDP ports and monitor remote access/RDP logs.
- Require administrator credentials to install software.
- Audit user accounts with administrative or elevated 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 virtual private network (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).

Additional Resources

For additional resources related to the prevention and mitigation of ransomware, go to Stopransomware.gov, a centralized, U.S. whole-of-government webpage providing ransomware resources and alerts.

CISA's Ransomware Readiness Assessment (RRA) is a no-cost self-assessment based on a tiered set of practices to help organizations better assess how well they are equipped to defend and recover from a ransomware incident.

CISA offers a range of no-cost cyber hygiene services to help critical infrastructure organizations assess, identify, and reduce their exposure to threats, including ransomware. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

Reporting Notice

The FBI encourages recipients of this document to report information concerning suspicious or criminal activity to their local FBI field office. Field office contacts can be identified at www.fbi.gov/contact-us/field-offices. When available, each report submitted should include the date, time, location, type of activity, number of people, and type of equipment used for the activity, the name of the submitting company or organization, and a designated point of contact.

Administrative Note

This product is marked **TLP:WHITE**. Subject to standard copyright rules, the information in this product may be shared without restriction.