FBI warns of ransomware attacks targeting US agriculture sector

By
Sergiu Gatlan (https://www.bleepingcomputer.com/author/sergiu-gatlan/)

April 20, 2022 03:13 PM **0**

The US Federal Bureau of Investigation (FBI) warned Food and Agriculture (FA) sector organizations today of an increased risk that ransomware gangs "may be more likely" to attack them during the harvest and planting seasons.

While ransomware groups regularly target the US agriculture sector, the FBI noted that the number of attacks against such entities during such critical seasons stands out.

The FBI revealed this in a joint flash alert released on Wednesday in coordination with the United States Department of Agriculture (USDA) and the Cybersecurity and Infrastructure Security Agency (DHS/CISA).

Top Articles
U.S. Treasury sanctions Russian cryptocurrency mining companies

Ransomware attacks targeting agricultural cooperatives during key seasons could lead to operation disruptions, financial loss, and a negative impact on the US and global food supply chain.

"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," the FBI said [PDF (https://www.ic3.gov/Media/News/2022/220420-2.pdf)].

"Cyber actors may perceive cooperatives as lucrative targets with a willingness to pay due to the time-sensitive role they play in agricultural production."

In today's private industry notification, the FBI highlighted several ransomware attacks against US agricultural cooperatives that led to financial losses and/or production impact:

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

Ransomware hits US critical infrastructure

In a February joint advisory (https://www.cisa.gov/uscert/ncas/alerts/aa22-040a), the FBI, CISA, and the NSA also highlighted an increase in ransomware incidents impacting 14 of the 16 US critical infrastructure sectors, including Food and Agriculture.

Since the start of the year, the FBI issued flash alerts highlighting how several ransomware gangs, including BlackByte (https://www.bleepingcomputer.com/news/security/fbi-blackbyte-ransomware-breached-us-critical-infrastructure/), Ragnar Locker (https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/), and Avoslocker (https://www.bleepingcomputer.com/news/security/fbi-avoslocker-ransomware-targets-us-critical-infrastructure/), have breached dozens of

Attackers use various methods to gain access to their victims' networks, such as phishing, stealing or brute forcing Remote Desktop Protocols (RDP) credentials, and exploiting unpatched vulnerabilities.

Ransomware gangs also employ cybercriminal services-for-hire to negotiate ransom payments, help victims make payments, and arbitrate payment disputes with other cybercriminals.

"If the ransomware criminal business model continues to yield financial returns for ransomware actors, ransomware incidents will become more frequent," the advisory said (https://www.cisa.gov/uscert/ncas/alerts/aa22-040a).

"Every time a ransom is paid, it confirms the viability and financial attractiveness of the ransomware criminal business model."

Related Articles:

FBI: BlackCat ransomware breached at least 60 entities worldwide (https://www.bleepingcomputer.com/news/security/fbi-blackcat-ransomware-breached-at-least-60-entities-worldwide/)

FBI: Avoslocker ransomware targets US critical infrastructure (https://www.bleepingcomputer.com/news/security/fbi-avoslocker-ransomware-targets-us-critical-infrastructure/)

FBI: Ransomware gang breached 52 US critical infrastructure orgs (https://www.bleepingcomputer.com/news/security/fbi-ransomware-gang-breached-52-us-critical-infrastructure-orgs/)

US warns of govt hackers targeting industrial control systems (https://www.bleepingcomputer.com/news/security/us-warns-of-govt-hackers-targeting-industrial-control-systems/)

FBI warns election officials of credential phishing attacks (https://www.bleepingcomputer.com/news/security/fbi-warns-election-officials-of-credential-phishing-attacks/)