Written by **Michael Tennant** on September 24, 2021

Hackers Demand $5.9 Million From Iowa Farm Cooperative in Ransomware Attack

A major Iowa farm cooperative was hit with a ransomware attack last weekend, with the hackers demanding $5.9 million in ransom.

skodonnell/iStock/Getty Images Plus

Fort Dodge-based NEW Cooperative provides agricultural services including feed supply and soil mapping throughout the Hawkeye State. Many of its services are computer-based, so an attack on its digital infrastructure could be devastating not just to the co-op itself but also to the world's food supply.

In an exchange with BlackMatter, the ransomware group that attacked its systems, NEW Cooperative said its software was behind 40 percent of grain production and the feeding schedules of 11 million animals. "If we are not able to recover very shortly, there is going to be very very public disruption to the grain, pork and chicken supply chain," the co-op asserted.

BlackMatter was unmoved by this plea. The group says it won't attack "critical infrastructure" such as hospitals, power plants, and government agencies, but it said it does not believe NEW Cooperative qualifies as critical. "The volumes of their production do not correspond to the volume to call them critical," BlackMatter told Bloomberg News via its dark web page. Moreover, "this company only works in one state." But what a state! Iowa is the nation's number-one corn producer and number-two soybean producer.

According to BleepingComputer, BlackMatter claims "to have stolen the source code for the soilmap.com project, R&D results, sensitive employee information, financial documents, and an exported database for the KeePass password manager."

BlackMatter told NEW Cooperative that it will only give the company a decryption tool to unlock its systems if the hackers are paid $5.9 million by September 25. However, "these ransom demands are a starting point for negotiations and usually lead to significantly smaller payments if a victim decides to pay," noted BleepingComputer.

"NEW Cooperative recently identified a cybersecurity incident that is impacting some of our company's devices and systems. Out of an abundance of caution, we have proactively taken our systems offline to contain the threat, and we can confirm it has been successfully contained," the co-op said in a statement. "We also quickly notified law enforcement and are working closely with data security experts to investigate and remediate the situation."

Meanwhile, according to Bloomberg, NEW Cooperative is temporarily using pre-digital methods to

ensure that feed and grain deliveries continue, though such methods are considerably slower than the computerized ones the firm had been employing.

BlackMatter is believed to be a Russian organization, quite possibly the successor to the DarkSide ransomware group that attacked the Colonial Pipeline in May. Its assault on NEW Cooperative is likely to raise the ire of President Joe Biden, who warned Russian President Vladimir Putin in July not to let hackers attack U.S. critical infrastructure, including food and agriculture. It will also test the ability of the Cybersecurity and Infrastructure Security Agency (CISA) to deal with ransomware attacks in light of Biden's declaration.

The NEW Cooperative attack is the just the latest in a long line of food-producer hackings in recent months. Ransomware expert Allan Liska told the Associated Press in June that "at least 40 food companies have been targeted by hackers over the last year." JBS, the world's largest meat processor, was subjected to a ransomware attack in May; the company ultimately paid $11 million to get its systems working again. Minnesota's Crystal Valley Cooperative was hit with ransomware this month.

The agricultural sector is particularly vulnerable to such attacks because many farmers "rely on farm platforms that can connect information from their tractors, drones, satellites, soil samples, and public sources to map out plans for planting, which herbicides or pesticides to use, and harvests," reported The Record. While this helps "improve yields, it can also expose farms' digital attack surfaces while creating a treasure trove of valuable data."

For now, hackers merely seem interested in filthy lucre, but that could change — for the worse — at any time, Rian Wanstreet, who studies agriculture and technology, told The Record.

"In some ways, we are lucky that the current focus is simply extortion: at some point, a hacker is going to act maliciously to misread temperature gauges, DDoS [distributed denial-of-service] a smart tractor fleet, or overprescribe/underprescribe fertilizers/chemicals," Wanstreet said. "Such disruptions would be catastrophic."