US farmer cooperative hit by $5.9M BlackMatter ransomware attack

By Lawrence Abrams

Published: 2021-09-20 · Archived: 2026-04-05 16:37:07 UTC

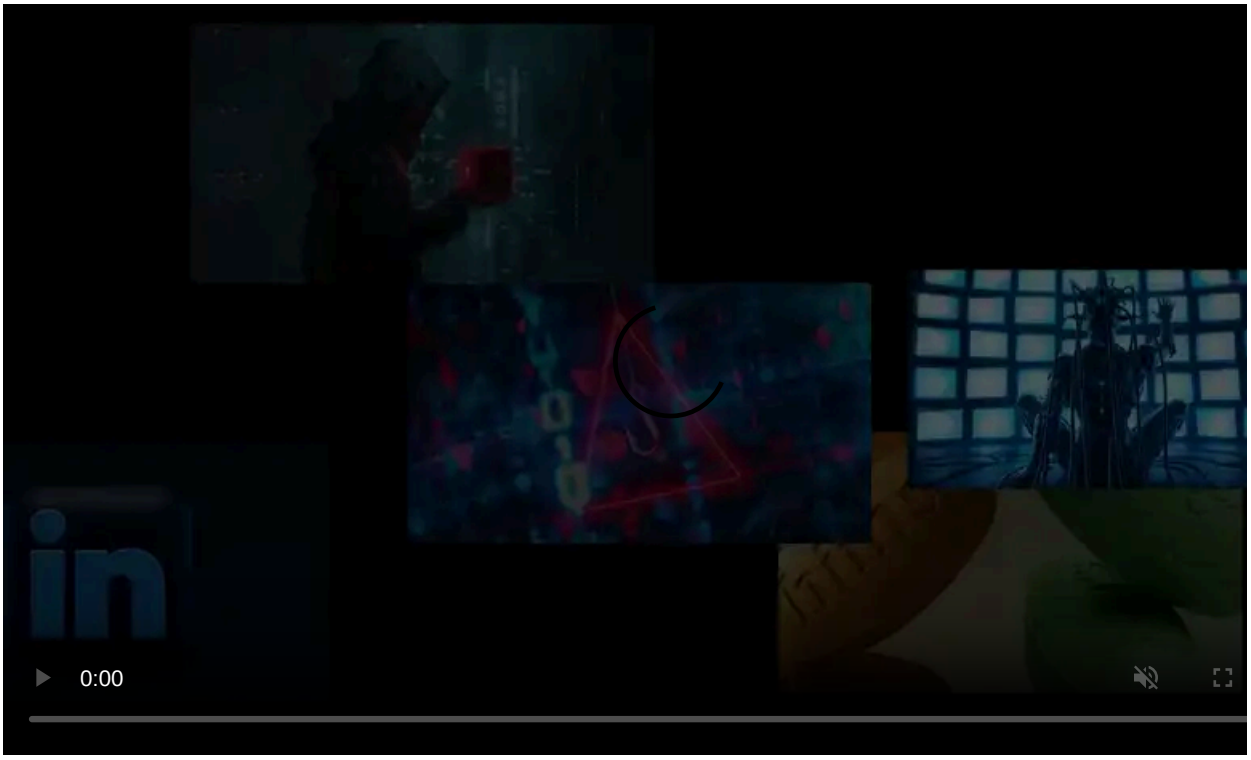
Source: newcoop.com

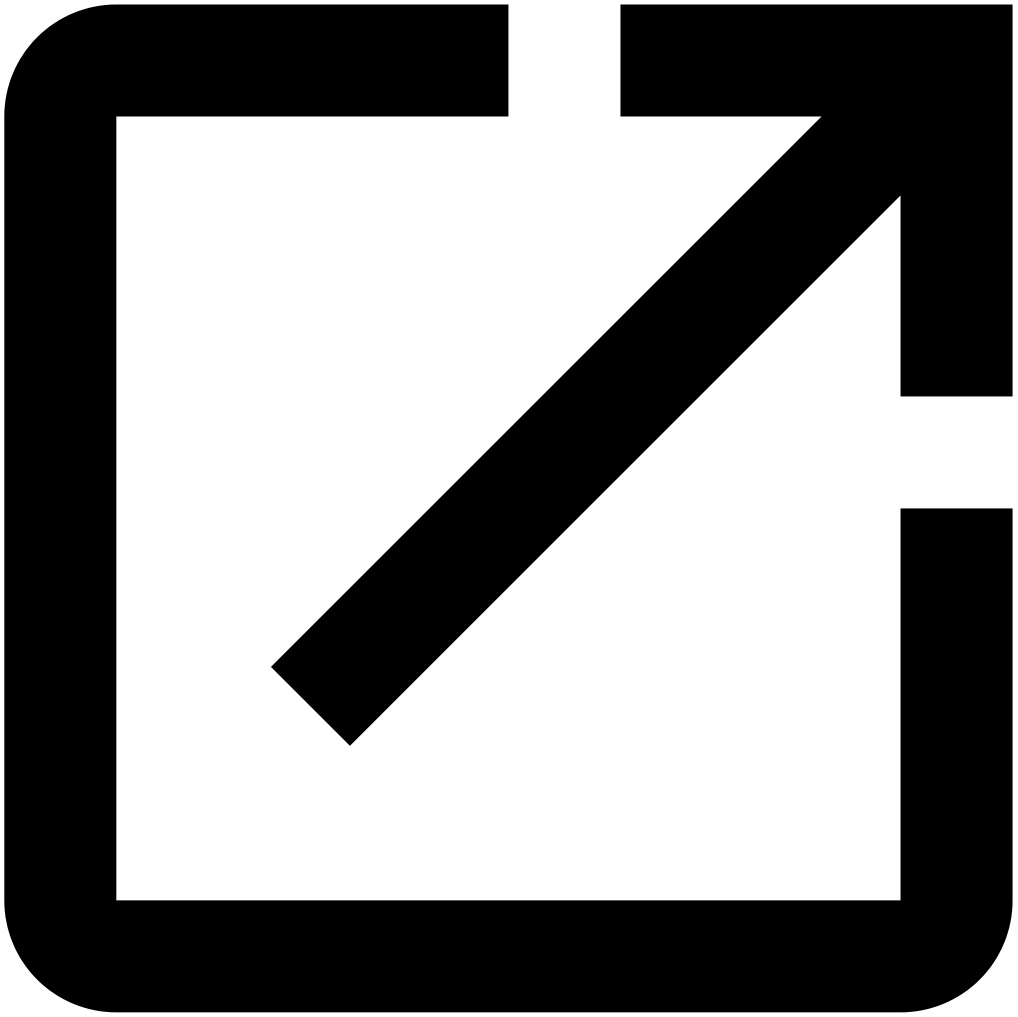
U.S. farmers cooperative NEW Cooperative has suffered a BlackMatter ransomware attack demanding $5.9 million not to leak stolen data and provide a decryptor.

NEW Cooperative is a farmer's feed and grain cooperative with over sixty locations throughout Iowa.

In a weekend ransomware attack, the threat actors demand a 5.9 million dollar ransom, which will increase to $11.8 million if a ransom is not paid in five days.

These ransom demands are a starting point for negotiations and usually lead to significantly smaller payments if a victim decides to pay.


0:00



NEW Cooperative has confirmed the attack to BleepingComputer and stated that they had taken their systems offline to contain the attack's spread.

“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," a NEW Cooperative spokesperson told BleepingComputer.

"We also quickly notified law enforcement and are working closely with data security experts to investigate and remediate the situation."

BlackMatter targets critical infrastructure

Researchers first learned of the attack after a ransomware sample was uploaded to a public malware analysis site early this morning.

This sample allowed access to the BlackMatter ransom note, the ransomware negotiation page, and a non-public data leak page containing screenshots of allegedly stolen data.

BlackMatter is believed to be a rebrand of the DarkSide ransomware that disappeared after attacking the Colonial Pipeline.

When BlackMatter first appeared, they stated that they would not target "Critical infrastructure facilities (nuclear power plants, power plants, water treatment facilities)."

From screenshots of the negotiation page shared on Twitter, NEW Cooperative asked BlackMatter why they were attacked as they are considered critical infrastructure and the attack will lead to food supply disruption for grain, pork, and chicken.

NEW Cooperative also said that they would have to contact regulators and CISA about the attack.

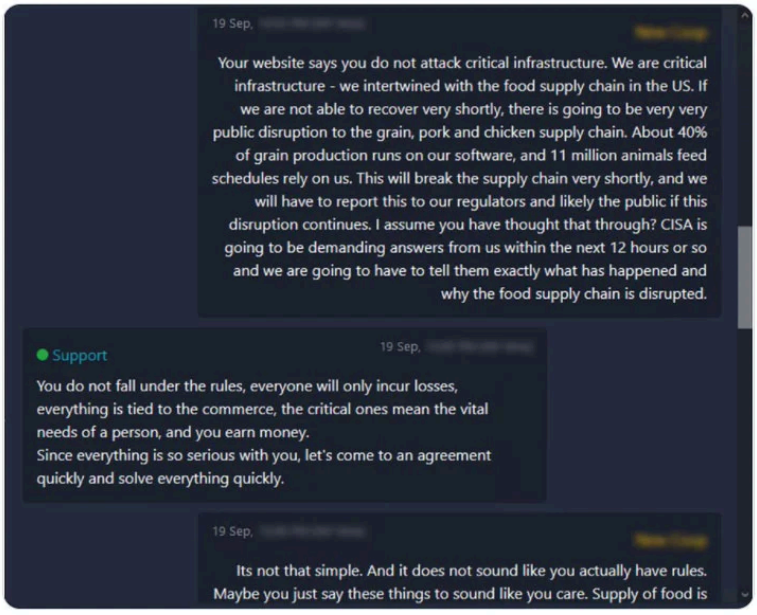
BlackMatter responded that they do not "fall under the rules" and threatened to double the ransom if NEW Cooperative didn't change their approach to the negotiation.

DarkFeed
@ido_cohen2

🌐 BlackMatter #Ransomware group just ransomed another food critical infrastructure in the US, The ransom demand is 5,900,000$ for now 🚨

The victim is playing by the rules: "@CISAgov is going to be demanding answers from us within the next 12 hours" 🧐

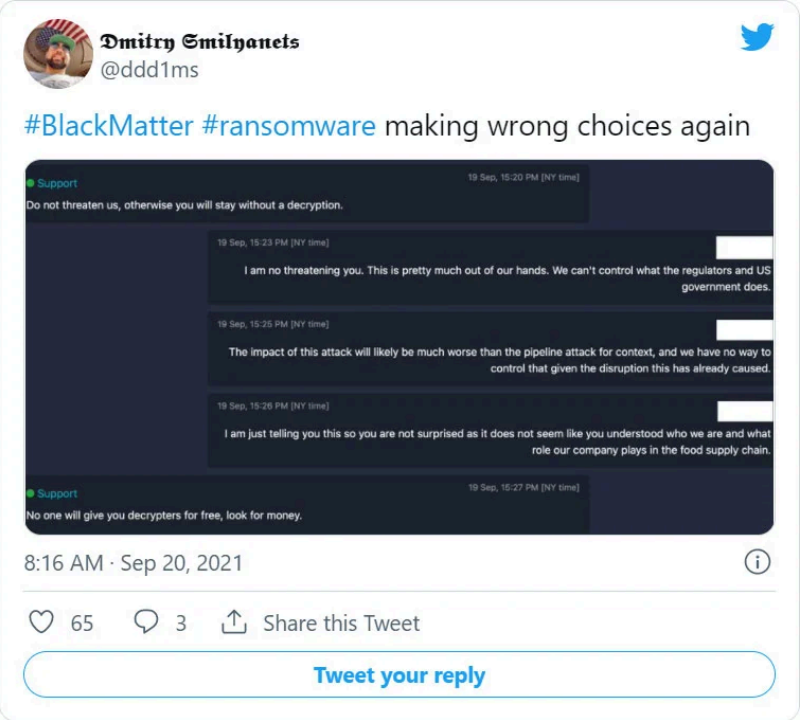
#BlackMatter



4:06 AM · Sep 20, 2021

319 12 Share this Tweet

Tweet your reply



"I am no threatening you. This is pretty much out of our hands. We can't control what the regulators and US government does," a NEW Cooperative representative told the threat actors in the negotiation chat.

"The impact of this attack will likely be much worse than the pipeline attack for context, and we have no way to control that given the disruption this has already caused."

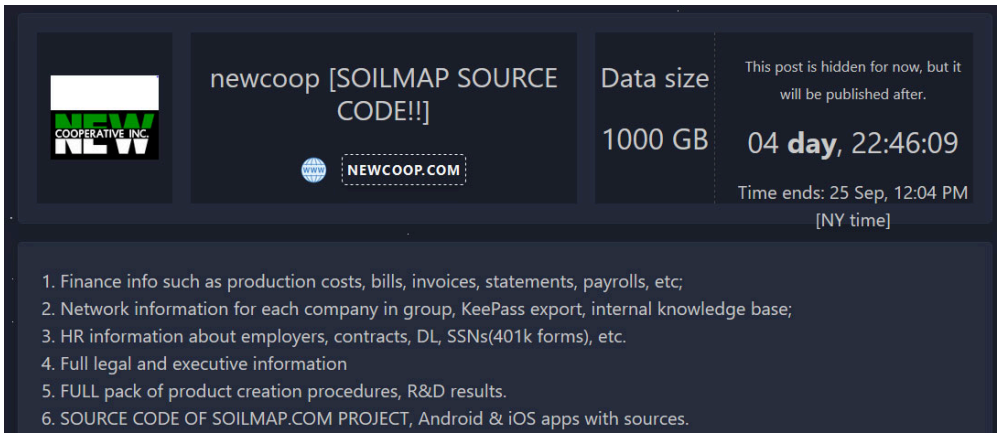
"I am just telling you this so you are not surprised as it does not seem like you understood who we are and what role our company plays in the food supply chain."

BlackMatter responded with, "No one will give you decrypters for free, look for money."

If you have first-hand information about this or other unreported cyberattacks, you can confidentially contact us on Signal at +16469613731, Wire at @lawrenceabrams-bc, or on Jabber at lawrence.abrams@anonym.im.

Threat actors claim to steal 1,000 GB of data

On the non-public data leak page, the threat actors claim 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.



Non-public data leak page for NEW Cooperative

The page includes screenshots of allegedly stolen data, including legal documents, a screenshot of an application, and financial information.

BleepingComputer has decided not to disclose these images due to their potentially sensitive nature.

Source: https://www.bleepingcomputer.com/news/security/us-farmer-cooperative-hit-by-59m-blackmatter-ransomware-attack/