HEADQUARTERS
CYBERSPACE SECURITY GROUP
COMMUNICATIONS, ELECTRONICS AND INFORMATION SYSTEMS SERVICE
ARMED FORCES OF THE PHILIPPINES
Camp General Emilio Aguinaldo, Quezon City

Sinclair Confirms Ransomware Attack That Disrupted TV Stations

A major cyberattack resulted in data being stolen, too, but Sinclair's not sure which information is now in the hands of the crooks.

Sinclair Broadcast Group, which owns hundreds of local television stations across the U.S., confirmed Monday that it has suffered a ransomware attack. The incident is disrupting its advertising operations, among other things, and spread to many of its owned TV affiliates over the weekend, knocking local broadcast feeds off the air.

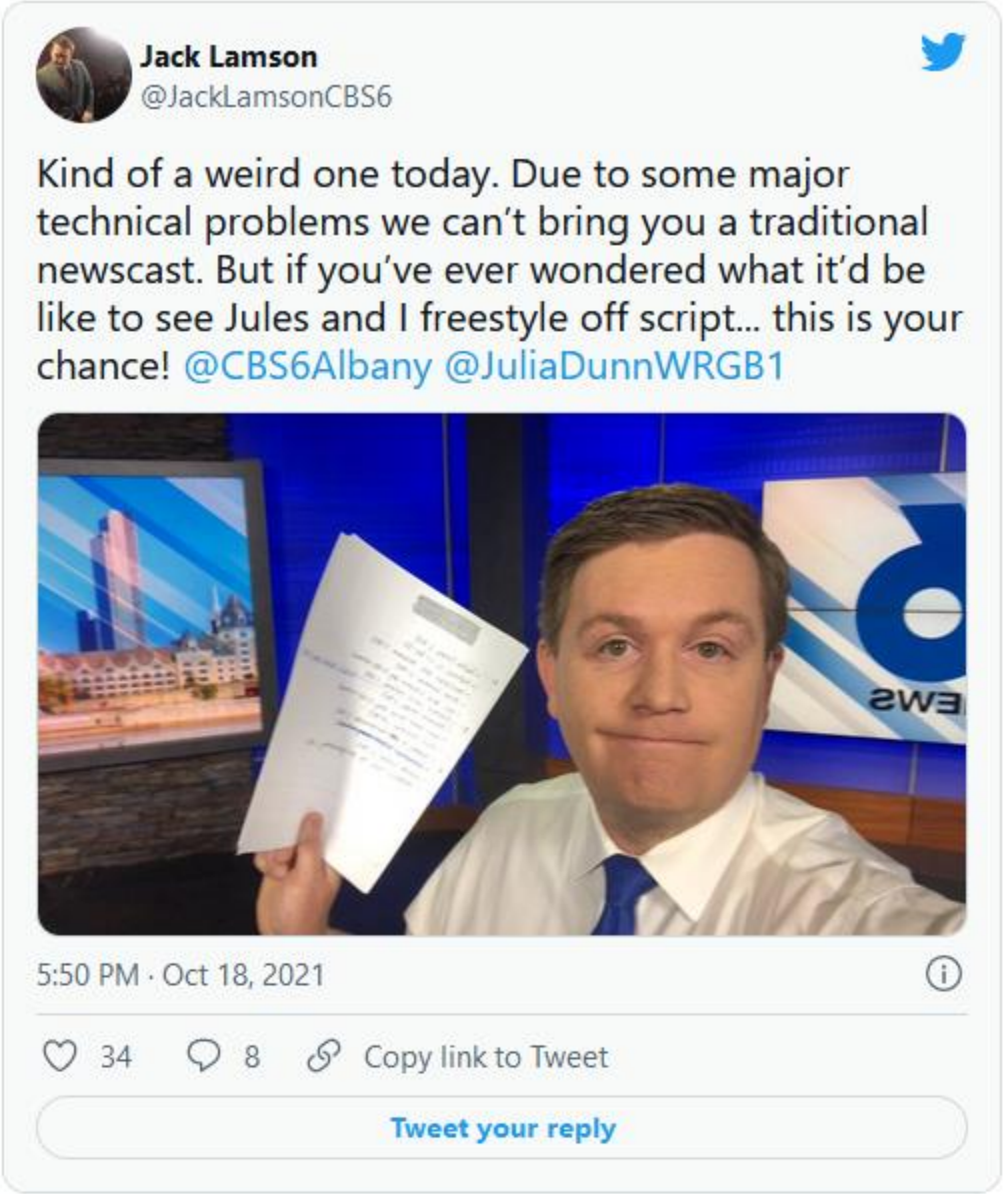
The cyberattack disrupted the company's general and office operations and resulted in data exfiltration, according to the media group's statement to the Securities and Exchange Commission (SEC):

"On October 16, 2021, the company identified and began to investigate and take steps to contain a potential security incident. On October 17, 2021, the company identified that certain servers and workstations in its environment were encrypted with ransomware, and that certain office and operational networks were disrupted."

Sinclair is "actively managing" the fallout from the attack, it said, after implementing its incident-response plan. "The forensic investigation remains ongoing," it added, explaining that it's dealing with continuing disruption, including problems with provisioning local commercials at its TV stations.

“Modern ransomware actors have learned to target an organization’s critical business systems as these need to be back online quickly and one of the easiest ways is to pay the ransom to obtain the key to decrypt those systems,” Jon Clay, vice president of threat intelligence at Trend Micro, said via email. “In this situation, targeting customers of the victim (local advertisers) by taking their revenue opportunities away could ensure the ransom is paid in order to get these systems back online quickly.”

Many of Sinclair’s 294 television stations took to Twitter on Sunday to let viewers know that they were experiencing technical difficulties – preventing their ability to provide local programming like news and other broadcast content like in-market NFL games.



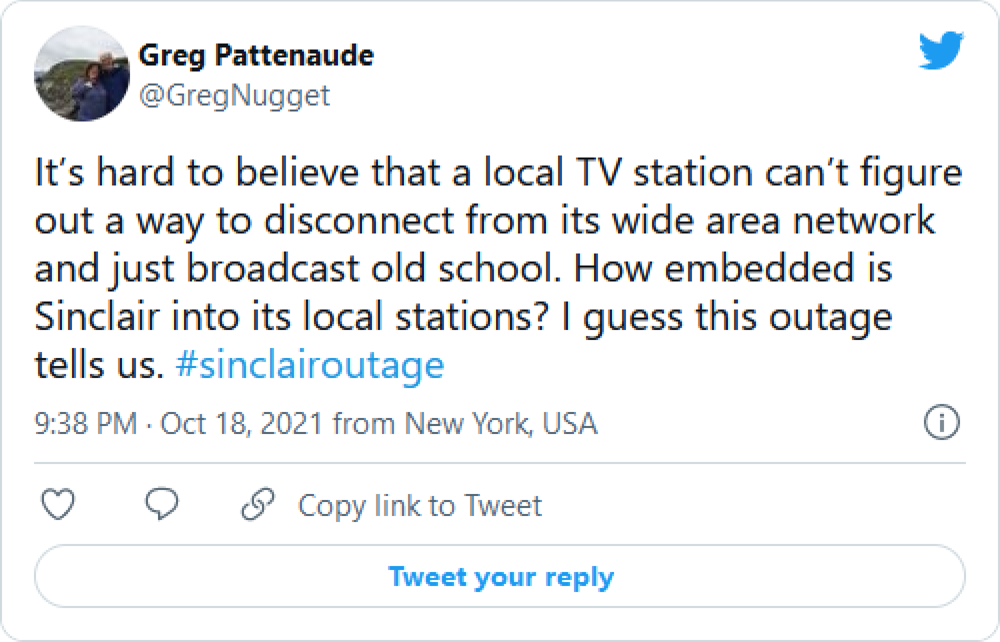
Jack Lamson
@JackLamsonCBS6

Kind of a weird one today. Due to some major technical problems we can’t bring you a traditional newscast. But if you’ve ever wondered what it’d be like to see Jules and I freestyle off script... this is your chance! @CBS6Albany @JuliaDunnWRGB1

5:50 PM · Oct 18, 2021

As of Monday, many had resumed operations, but some are still dealing with some lingering issues such as trouble using weather graphics, according to reports.

A source also told the Record that the stations are interconnected by a central Sinclair Active Directory, which allowed the cyberattackers to infiltrate seemingly disparate operations. However, they failed to reach a network area known as “the master control,” which allowed Sinclair to provide a working national feed to affected stations, according to the source.



Greg Pattenaude
@GregNugget

It’s hard to believe that a local TV station can’t figure out a way to disconnect from its wide area network and just broadcast old school. How embedded is Sinclair into its local stations? I guess this outage tells us. #sinclairoutage

9:38 PM · Oct 18, 2021 from New York, USA

Another issue is the data that was stolen. Sinclair confirmed that data was taken, but it’s not yet sure which information the attackers have. “The company will take other actions as appropriate based on its review,” it said.

Sinclair didn’t supply other details that would be of interest, such as which ransomware strain was used, how the ransomware infiltrated its network initially or a timeline for remediation. However, the company added that it’s reviewing security protections for areas of improvement, which is probably a good idea, according to researchers.

“It should be noted that even though threat actors deployed ransomware just a few days ago, with many ransomware attacks these days, the initial access that precipitated the attack generally occurs weeks, if not months, ahead of time,” said Crane Hassold, director of threat intelligence at Abnormal Security, via email. “This initial foothold, which could be caused by a separate malware infection or vulnerable web application, is what is exploited to deploy the ransomware.”

Garret Grajek, CEO, YouAttest, noted that a successful attack on a major media player should be of utmost concern.

“Penetration of all our key systems, water, energy, transportation and media is a grave concern for western countries,” he said via email. “The fact that a major media outlet like Sinclair was affected shows how vulnerable even those with security resources are to cyberattacks. Enterprises need to go beyond just password resets and even 2FA [two-factor authentication] and start understanding the scope and capabilities of all the identities in their enterprises."

He added, "This means practicing the principle of least privilege to [ensure] that all accounts, especially when they are compromised, do not have access to resources they do not need access to but could inflict damage if the account falls under control of [a] malicious party. User accounts are easily stolen and guessed by the hackers, which then conduct lateral movement across the enterprise and privilege escalation to obtain access to valued resources. Enterprises must be aware of the rights granted and triggered when privileges are modified."

References:

https://threatpost.com/sinclair-ransomware-tv-stations/175548/

https://therecord.media/sinclair-tv-stations-disrupted-across-the-us-in-apparent-ransomware-attack/

https://www.chroniclejournal.com/business/national_business/sinclair-hit-by-ransomware-attack-tv-stations-disrupted/article_a0ba2d08-25a9-5308-a8ac-6d7d43ab8cb7.html

https://www.mysanantonio.com/entertainment/article/Sinclair-Broadcast-Group-identifies-data-breach-16541810.php

https://www.reuters.com/technology/us-tv-station-operator-sinclair-hit-by-ransomware-attack-2021-10-18/

https://www.pcmag.com/news/ransomware-hits-sinclair-broadcast-group-disrupts-tv-stations

https://www.engadget.com/sinclair-broadcast-group-ransomware-attack-154239001.html

https://abcnews.go.com/Entertainment/wireStory/sinclair-broadcast-group-identifies-data-breach-80640053

https://www.govinfosecurity.com/sinclair-tv-stations-targeted-in-weekend-ransomware-attack-a-17753