City of Tulsa's online services disrupted in ransomware incident

bleepingcomputer.com/news/security/city-of-tulsas-online-services-disrupted-in-ransomware-incident/

Lawrence Abrams

By
Lawrence Abrams

- May 10, 2021
- 05:27 PM
- 0

The City of Tulsa, Oklahoma, has suffered a ransomware attack that forced the City to shut down its systems to prevent the further spread of the malware.

Tulsa is the second-largest city in Oklahoma, with a population of approximately 400,000 people.

Over the weekend, threat actors deployed a ransomware attack on the City of Tulsa's network that led to the City shutting down all of its systems and disrupting online services.

"We identified malware on our servers and as soon as we did that, in an abundance of caution, we shut all of our systems down." Tulsa Mayor GT Bynum told local media KRMG in an interview.

Bynum says that employees are back to work, and the incident did not affect 911 services or emergency response.

However, the shutdown of City systems is preventing residents from accessing online bill payment systems, utility billing, and services through email. Websites for the City of Tulsa, the Tulsa City Council, Tulsa Police, and the Tulsa 311 websites are also down for maintenance.

The City's phone systems are up and running, and anyone who needs to conduct business with the City can do so over the phone.

In a Facebook post, the City states that customer information has not been compromised. As most ransomware operations steal data before deploying their ransomware, some amount of files was stolen.

"The City of Tulsa is experiencing technical difficulties on many outward facing programs that help serve the citizens of Tulsa due to a ransomware attack. No customer information has been comprised, but residents will not be able to access City websites and there will be delays in network services," says a post to the Tulsa Police Department's Facebook page.

Ransomware has become a scourge on US interests, with new attacks disclosed daily and victims paying million-dollar ransoms.

To help combat the increasing threat of ransomware, a Ransomware Task Force has been created to analyze the problem and provide recommended solutions to lawmakers.

These solutions range from mandatory disclosure of ransom payments to an internationally coordinated effort to help organizations prevent and respond to ransomware attacks.

Attacks on critical infrastructure have also become a significant concern in light of last week's cyberattack on the largest US fuel pipeline by the DarkSide ransomware gang.

Related Articles:

Costa Rica declares national emergency after Conti ransomware attacks

New Black Basta ransomware springs into action with a dozen breaches

American Dental Association hit by new Black Basta ransomware

Wind turbine firm Nordex hit by Conti ransomware attack

Hackers use Conti's leaked ransomware to attack Russian companies

- Cyberattack
- Oklahoma

- Ransomware
- Tulsa

Lawrence Abrams

Lawrence Abrams is the owner and Editor in Chief of BleepingComputer.com. Lawrence's area of expertise includes Windows, malware removal, and computer forensics. Lawrence Abrams is a co-author of the Winternals Defragmentation, Recovery, and Administration Field Guide and the technical editor for Rootkits for Dummies.

- Previous Article
- Next Article

You may also like: