Ryuk Ransomware Campaign Targets Port Lavaca City Hall

By CISOMAG

Published: 2020-02-18 · Archived: 2026-04-05 17:28:08 UTC

The Port Lavaca City Hall's server was recently hit by Ryuk ransomware that apparently entered through the email system. The ransomware took down the local government's server, the city's billing and auto-pay systems, and disrupted other regular operations. However, water, sewer, and the police department's systems remained unaffected in the incident.

According to the City's Mayor Jack Whitlow, no information was stolen or compromised but the attackers encrypted the files to demand a ransom. The city officials are working on restoring their systems to get back into working order. It's said that the attack already incurred a bill amounting to nearly US$50,000 to the City. Whitlow stated that hackers demanded US$200,000 ransom to decrypt the data.

The City officials reported the issue to the FBI for further investigation and confirmed that they're not fulfilling any ransom demands. Whitlow said, "I'd rather pay the people in town to fix it and keep the money in the community. We're going to be down for a little while. It may take a while to get completely up to date. We are getting most of our system up and running, but we are recovering some of that data right now."

The Port Lavaca City Hall's Manager William DiLibero stated, "The attack brought down our billing system. Our online and auto payment systems are out of service and we have gone back to our older collection and payment

processes. Staff are collecting cash, check and credit card payments at City Hall. We will need to rebuild our database in order to get the payment system back to full operational status. The City has worked with State and Federal agencies to address this attack."

Ryuk in the News

Recently, the officials of the U.S. Coast Guard (USCG) disclosed a Ryuk ransomware infection that took down the entire corporate IT network of a Maritime Transportation Security Act (MTSA) regulated facility for more than 30 hours. According to the USCG officials, the ransomware interrupted the camera and physical access control systems. It's believed that a malicious email sent to one of the maritime facility's employees was the entry point for the ransomware infection.

The ransomware corrupted the enterprise IT network files, encrypted them, and prevented the facility's access to critical files. The officials stated that the incident affected the facility's IT network and industrial control systems that monitor and control cargo transfer operations.
