Florida city mum on ransom demands by cyberattackers

14 December 2019, by Bobby Caina Calvan and Frank Bajak

A Florida city confirmed Friday that hackers seeking to extort money were responsible for crippling its computer systems earlier this week but officials have yet to decide whether they will pay a reported $1 million ransom.

If they do opt to fork over the money, they may have to dip into Pensacola city coffers; the city of about 52,000 in Florida's Panhandle—whose annual budget is roughly $245 million—is not insured for such an attack.

Obtaining it in the future is "something that our risk manager will certainly be looking into," said city spokeswoman Kaycee Lagarde.

Lagarde confirmed that ransomware was behind the attack that brought down the city's computer network over the weekend, less than a day after a Saudi aviation student killed three U.S. sailors and wounded eight other people at a nearby naval air station.

The FBI has said the attacks were not connected.

The cybersecurity blog BleepingComputer reported earlier this week that a group behind a ransomware strain known as Maze claimed responsibility for the attack and was demanding $1 million from the city.

In emails exchanged with the website, the Maze hackers claimed they had stolen documents from the city but didn't say whether they had given Pensacola officials a deadline to pay for them or if they had threatened to release the documents if they didn't pay. Ble epingComputer editor Lawrence Abrams said the Maze operators had authenticated their identity with proof of a different hack and by posting snippets of email exchanges with his blog on a dark-web payment site.

City officials declined to discuss who might have been responsible or any ransom amount demanded against the city. The city said it has restored some services, including email, phone services and utility online bill payments.

Ransomware infections reached epidemic dimensions this year, and security researchers are concerned ransomware could also disrupt next year's U.S. presidential elections.

According to a new report released this week by the cybersecurity firm Emsisoft, more than 948 U.S. government agencies, educational institutions and health care providers were hit in an unprecedented barrage at a potential cost of more than $7.5 billion.

New Jersey's largest hospital system and the city of New Orleans are among the most recent U.S. ransomware victims.

Hackensack Meridian Health, which operates 17 hospitals and other facilities, said Friday that it paid an undisclosed amount to regain control over systems disrupted last week— and that it had insurance for such emergencies.

In New Orleans, investigators discovered ransomware as they looked into a suspected cyberattack that led to a shutdown of city computers on Friday. City officials said they had not received a ransom demand, however, and it was initially unclear whether the attack did any damage to the city's system.

In May, a cyberattack hobbled Baltimore's computer network and cost the city more than $18 million to repair. City officials refused to pay demands for $76,000 in bitcoin.

During the summer, two Florida cities—Riviera Beach and Lake City—paid hackers more than $1 million combined after being targeted.

Pensacola officials became aware of the cyberattack against their city about 1:30 a.m.

Saturday.

Ever since, information technology technicians have been working to restore services as city officials continued to take stock of the damage, if any, and determine what information might have been compromised or stolen by the hackers.

Lagarde would not say whether any personal or financial data was breached. She said the city would notify residents and customers as warranted.