Submitted by staff at 9/9/2019 Meeting
Item 2

NATIONAL

22 Texas Towns Hit With Ransomware Attack In 'New Front' Of Cyberassault

LISTEN · 3:37 PLAYLIST Download

Transcript

August 20, 2019 · 10:16 AM ET
Heard on Morning Edition

BOBBY ALLYN

Texas state Capitol building in Austin. This week, state officials confirmed that 22 municipalities have been infiltrated and ransom demanded.

Bill Clark/CQ-Roll Call/Getty Images

Updated at 10:00 a.m. Wednesday ET

Texas is the latest state to be hit with a cyberattack, with state officials confirming this week that computer systems in 22 municipalities have been infiltrated by hackers demanding a ransom. A mayor of one of those cities said the attackers are asking for $2.5 million to unlock the files.

The Federal Bureau of Investigation and state cybersecurity experts are examining the ongoing breach, which began Friday morning and has affected mostly smaller local governments. Officials have not disclosed which specific places are affected.

Investigators have also not yet identified who or what is behind the attack that took the systems offline, but the Texas Department of Information Resources says the evidence so far points to "one single threat actor."

Elliott Sprehe, a spokesman for the department, said he was "not aware" of any of the cities having paid the undisclosed ransom sought by hackers. He said the areas impacted are predominantly rural. The department initially put the number of cities attacked at 23.

Two cities so far have come forward to say their computer systems were affected. Officials in Borger in the Texas Panhandle, said the attack has affected city business and financial operations. Birth and death certificates are not available online, and the city can't accept utility payments from any of its 13,250 residents. "Responders have not yet established a time-frame for when full, normal operations will be restored," city officials said.

Article continues below

Keene, Texas, a city of some 6,100 people outside Fort Worth, was also hit, officials announced. The city's government is also unable to process utility payments.

Keene Mayor Gary Heinrich told NPR that the hackers broke into the information technology software used by the city and managed by an outsourced company, which he said also supports many of the other municipalities targeted.

"Well, just about everything we do at City Hall is impacted, Heinrich said.

Heinrich said the hackers want a collective ransom of $2.5 million.

"They got into our software provider, the guys who run our IT systems," Heinrich said. "A lot of folks in Texas use providers to do that, because we don't have a staff big enough to have IT in house."

State officials would not comment on the nature of the attack or confirm the ransom amount. But Heinrich said there is no way his city will be coughing up anything for the hackers.

"Stupid people," he said of the cyber-attackers. "You know, just no sense in this at all."

Experts say that while government agencies have increasingly been hit by cyberattacks, simultaneously targeting nearly two dozen cities represents a new kind of digital assault.

"What's unique about this attack and something we hadn't seen before is how coordinated attack this attack is," said threat intelligence analyst Allan Liska. "It does present a new front in the ransomware attack," he said. "It absolutely is the largest coordinated attack we've seen."

Liska's research firm, Recorded Future, has found that ransomware attacks aimed at state and local government have been on the rise, finding at least 169 examples of hackers breaking into government computer systems since 2013. There have been more than 60 already this year, he said.

In recent months, the data networks of Baltimore, the Georgia courts system and a county in Utah have all been hit by ransomware.

The hacker bait tends to come in the form of a seemingly benign email with links or attachments that, once opened, can infect a system. There are other popular ways of tapping into government networks, Liska said, like through remote desktop systems, which can be vulnerable to hackers.

While the attackers tend to be anonymous and their locations undisclosed, Liska said his research has found that few are based in the U.S. Many, he said, are breaching local government computer systems from operations based in parts of Eastern Europe or Russia.

And sometimes local governments see no other option to restoring their crippled networks than paying a ransom demanded by hackers. In Lake City, Fla., a town of about 12,000 residents, officials paid $460,000 in the form of bitcoin, the preferred payment method among cybercriminals.

"They turned off the servers. They literally went room through room through city hall, unplugging people's networks cables and turning off all the computers," Mike Lee, a sergeant with the Lake City Police Department, told NPR in July.

The ransom was paid by insurance, but taxpayers were still on the hook for a $10,000 deductible.

The Recorded Future study found that about 17% of local agencies hit with ransomware viruses paid up, a practice federal law enforcement officials discourage, saying it incentivizes cybercriminals to keep engaging in the activity.

Liska said in cities he has worked with that have been preyed upon by hackers, there are instances in which ponying up for the return of data is the only viable option.

"Sometimes the reality of the situation may call for it," he said. "If the backups aren't working or if the bad guys have encrypted your backups, then unfortunately that's what you're left with."

Individuals, businesses and institutions such as hospitals have been targeted by ransomware attacks for years. With the recent attacks on state and city government, local officials are rushing to secure their computer systems, holding new training and backing up their servers, Liska said. But in smaller, cash-strapped localities, there could be challenges to building a security defense.

Tad McGalliard studies local government cybersecurity at the Washington-based city manager group ICMA. He has been pushing for municipalities to find more funding to fight back against hackers.

"Somebody out there on the bad guy front is seeing an opportunity in local governments and we got to make a better job of making sure our employees are as well-trained and as well-equipped as possible," McGalliard said.

McGalliard said the Texas case should be a wake-up call to cities in remote parts of the country.

"We might have thought this was a big city problem, or at least an affluent city or county problem, but I think what's clear now is just about any local government is vulnerable," he said.

In Texas, state authorities have not yet disclosed where exactly the attacks were based or how many computers have been swept up in the breach, meaning it is not yet known what services or data might have been compromised.

"Hitting 23 towns at once was bad, but we don't know how much damage was done," Liska said. "One computer in each town versus 100 computers in each town is a big difference."

More Stories From NPR