The New York Times

A City Paid a Hefty Ransom to Hackers. But Its Pains Are Far From Over.

By Frances Robles

July 7, 2019

LAKE CITY, Fla. — Audrey Sikes, city clerk of Lake City, Fla., has a thing for documents: She does not like losing them.

It falls to Ms. Sikes, as official custodian of records for this city of 12,000 people about an hour west of Jacksonville, to maintain Lake City's archives. She keeps a log of public record requests and has spreadsheets that track things like property deeds and building permits. She spent years digitizing all the papers of a city that incorporated before the Civil War.

"It's everything I do," Ms. Sikes said.

Did.

More than 100 years' worth of municipal records, from ordinances to meeting minutes to resolutions and City Council agendas, have been locked in cyberspace for nearly a month, hijacked by unidentified hackers who encrypted the city's computer systems and demanded more than $460,000 in ransom.

Weeks after the city's insurer paid the ransom, the phones are back on and email is once again working, but the city has still not recovered all of its files. There is a possibility that thousands of pages of documents that had been painstakingly digitized by Ms. Sikes and her team will have to be manually scanned, again.

"It puts us years and years and years behind," Ms. Sikes said.

[Read more about the attack on Lake City.]

Lake City's troubles are hardly unique. In the past month alone, at least three Florida cities have been victims of ransomware attacks, after intrusions on larger cities such as Atlanta, Dallas and Baltimore.

What sets the latest cyberattacks apart is the stunning size of their ransom demands. Riviera Beach, Fla., last month agreed to pay more than $600,000, several times what was asked of Baltimore, which did not have insurance and did not pay. The Village of Key Biscayne, near Miami, has not publicly disclosed whether it plans to pay the perpetrators of a recent ransomware attack. Earlier this year Jackson County, Ga., paid $400,000.

Atlanta's mayor testified last week to Congress that an attack last year, when the city refused to pay $51,000 in extortion demands, has so far cost the city $7.2 million.

As cities rush to protect their data — and others scramble to recover it — experts on cybersecurity say the growing number of attacks and escalating ransom demands suggest that cyberattackers have found a ripe target: small governments with weak computer protections and strong insurance policies. The payments keep coming even as the F.B.I. says they might be incentivizing more attacks.

"It is quite profitable for the actors to conduct these sorts of attacks on victims," Adam Lawson, a supervisory special agent for the F.B.I.'s cyber division, said in an interview. "At the end of the day, people are paying the ransoms."

The F.B.I. said it had received nearly 1,500 ransomware reports last year, a number the agency acknowledges does not begin to reflect the size of the problem, in part because some private institutions may decide to handle things quietly to avoid damage to their reputation. An Illinois computer programmer who offers free help decrypting ransomware said the automated website he designed, ID Ransomware, receives 1,500 requests for assistance every day. Hospitals, businesses and other networks have been attacked for years, but the new wave of ransomware directed at government agencies has made them much more visible to the public.

Cities, in response, are rushing to beef up their backup systems and train employees to avoid malicious spearphishing emails, the most common means of attack, in which hackers send an innocuous-looking email with an attachment or link that spreads the malicious code. In Lake City, a new cloud-based backup system is expected to cost $60,000 a year.

City employees there first noticed troubles on June 6, when the city's computer systems went down briefly, then came up again, Ms. Sikes said. Four days later, when employees sat down at their desks at 7:30 a.m., the computers did not work and neither did the telephones. Even cellphones were wiped of contacts.

Information technology technicians who tried to open files on the city's servers were greeted with a message: "How do you want to open this type of file?" It was accompanied by two unfamiliar email addresses.

"Balance of shadow universe," the mysterious pop-up concluded.

I.T. workers began rushing through the building, urging employees to unplug their computers — both the Ethernet and power cables. They got on their cellphones to direct workers in satellite facilities to do the same.

It was too late, though.

The city had fallen victim to what is called a triple-threat Ryuk attack, which is usually spread through spearphishing emails. The city does not know who clicked on what attachments, and said it could not disclose some information because of a pending F.B.I. investigation.

Nearly all of the city's systems — including its water and gas payment systems — were unusable. The copy machines, also linked to the computer network, did not work. There was no email. The phones were down.

The searchable database that Ms. Sikes and her team had spent so long setting up, which allowed city workers and the public to look up everything from deeds to permits and city resolutions on any topic of interest, was gone.

The intrusion was linked to a malware strain similar to the one used to target a North Carolina water utility last year.

When Lake City employees sat down at their desks at City Hall one morning last month, their computers and telephones did not work. I.T. workers began rushing through the

building, urging employees to unplug their computers. But it was too late.
Eve Edelheit for The New York Times

And from what the city's computer security people could tell, it would be impossible to circumvent. The city had backup files for all its data, but they were on the same network — and also inaccessible.

"We were running blind," said Stephen A. Roberts, the city's safety and risk management director. "It was scary. We were D.O.A. the entire day, trying to run the city like it was 1950."

Business that ordinarily would be done by email, or on a conference call, had to be done in face-to-face meetings, or using personal cellphones.

"The most impactful was the loss of the email," said Mike Lee, a spokesman for the police department. "That probably hit everybody in the city the hardest."

Residents who needed to pay their water or gas bills could do so only with cash or money orders. They were given handwritten receipts.

"When it first happened, a lot of people felt like, 'There's nothing to do, let's go home,'" Ms. Sikes said.

But no one was ready to give up that easily. A few computer terminals were set up at the police station, which, like the fire department, was on a separate server and unaffected by the malware attack. Employees printed out documents on their equipment at home.

"If you had to correspond with the city attorney, you had to get in the car and drive a document to him, or, turns out there is this thing called a fax machine that no one ever uses," Ms. Sikes said.

About 16 terabytes of information were effectively locked, said Joseph Helfenberger, the city manager. (One terabyte is 1,024 gigabytes.)

Days after the attack, a ransom demand arrived. It was shockingly high, city officials said. They declined to say exactly how much it was because the investigation is still underway.

The municipal records Ms. Sikes and her team spent years scanning are stored in a vault at city hall. Eve Edelheit for The New York Times

The city's insurer, the Florida League of Cities, hired a consultant to handle the negotiations with the hackers via the email addresses that had been posted on the city server.

The initial demands were refused outright, and city technicians raced to find a workaround. "We tried a lot of different solutions," said Mr. Helfenberger. None of them worked. "We were at the end of the day faced with either recreating the data from scratch, or paying the ransom," he said.

The insurer's negotiator settled on a payment of 42 Bitcoins, or about $460,000, Mr. Helfenberger said, of which the city would pay a $10,000 deductible.

After the payment, the hackers provided a decryption key, and recovery efforts began in earnest.

As it turned out, recovery would not be simple. Even with the decryption key, each terabyte has taken about 12 hours to recover. Much of the city's data, nearly a month after the onset of the attack, has still not been unlocked. "I thought it would be restored a lot sooner," Mr. Helfenberger said. "My entire career, the most I lost data was maybe three days."

Law enforcement officials worry that the vulnerability of cities like Lake City — and the hefty ransoms paid out in recent months — will encourage more attacks.

Mr. Lawson, of the F.B.I.'s cyber division, said the bureau's official position was that victims should not pay ransoms. But many city officials and computer network specialists say that cities often have no choice. The cost for recovering data can far surpass the ransom demand, and agencies often find themselves unable able to perform the most basic municipal tasks. In some cases, even emergency services have been affected.

[Cities are wrestling with whether to pay ransoms to hackers.]

"These groups are always trying to find that sweet spot: What is enough someone will consider paying but not so much that they'll say, 'Forget that. It's easier to rebuild,'" said Mark A. Orlando, the chief technology officer for Raytheon Intelligence Information and Services. "This is a situation where that amount is going up, and we have reached a new high-water mark as to what is getting paid out."