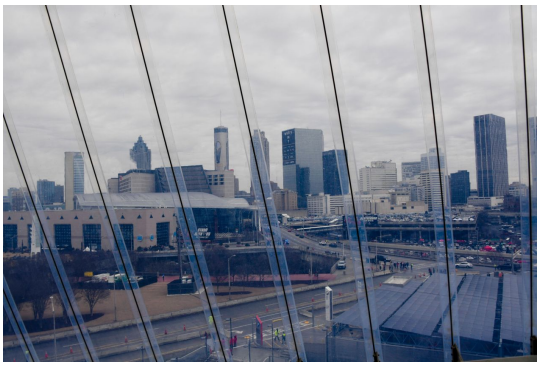
THE WALL STREET JOURNAL.

U.S.

Ransom Demands and Frozen Computers: Hackers Hit Towns Across the U.S.

Online extortionists search for vulnerabilities, offer instructions on how to pay in bitcoin



A view of the Atlanta skyline from inside Mercedes-Benz Stadium. PHOTO: JIM BROWN/NEWSCOM/ZUMA PRESS

By Jon Kamp and Scott Calvert
June 24, 2018 7:00 a.m. ET

Town officials in Rockport, Maine, were closing up shop on Friday, April 13, when they realized they couldn't open files on their computers.

After fielding messages from town workers, local information-technology contractor Gus Natale said he "went straight to the town office and started yanking plugs."

An unknown hacker had snuck malicious software onto the network and was demanding a payment of roughly $1,200 in bitcoin in return for codes to unlock the town's files.

"My thinking was, let's just get this paid. It's a small amount," said Town Manager Rick Bates. But, he added, Mr. Natale and a helper "did not want the bad guys to beat them."

The attack on Rockport is one example in a rising tide of similar invasions of municipal systems across the U.S.—from major cities like Atlanta, which got hit in March, to counties, tiny towns and even a library system in St. Louis. Local governments are forced to spend money on frantic efforts to recover data, system upgrades, cybersecurity insurance and, in some cases, to pay their online extortionists if they can't restore files some other way.

Public-sector attacks appear to be rising faster than those in the private sector, according to the Ponemon Institute, a Traverse City, Mich., research company focused on information security. Ponemon estimates 38% of the public entities it samples will suffer a ransomware attack this year, based on reports through May, up from 31% last year and 13% in 2016. The company samples roughly 300 to 400 public-sector entities each year.

"We're right at the front end of this," said Marshall Davies, executive director of the Alexandria, Va.-based Public Risk Management Association. Hackers are "just now coming after the public entities. They've been hitting the businesses for years," he said.

Hackers generally don't target specific cities, but instead are constantly searching for vulnerabilities wherever they may occur, security experts said. "The trick about ransomware right now is that it's typically not a targeted, focused attack," said Christopher Krebs, a senior official at the Department of Homeland Security, at a recent mayors' conference in Boston. "You're not special."

Hackers attacking cities aren't typically nation states, but rather cybercriminals, Mr. Krebs said. Sometimes the hackers demand ransoms in poorly written English, and they typically demand to be paid in bitcoin, according to officials who have been hacked. The Rockport hacker offered a "customer service" chat window and offered tips on how to acquire cryptocurrency.

The Federal Bureau of Investigation advises against paying, and warns that "some individuals or organizations are never provided with decryption keys after paying a ransom."

Rockport didn't pay the hackers. Instead, Mr. Natale and a helper worked through the weekend to recover files from a compromised backup server, and had town systems up and running again by the next week. Still, the hamlet of about 3,400 ultimately paid about $10,000 to cover the immediate restoration work, plus another $28,000 to $30,000 on security improvements, including a cloud-based backup system.

RANSOM REQUESTS

- Atlanta: March 2018. Ransom demanded: $51,000 (not paid)
- Leeds, Ala.: Feb. 2018. Ransom demanded: $12,000 (paid $8,000)
- Montgomery County, Ala.: Sept. 2017. Ransom demanded: $33,000 (paid in full)
- Rockport, Maine: April 2018. Ransom demanded: $1,200 (not paid)
- St. Louis Public Library: Jan. 2017. Ransom demanded: $25,000 (not paid)
- Licking County, Ohio: Early 2017. Ransom demanded: $50,000 (not paid)
- Spring Hill, Tenn.: Late 2017. Ransom demanded: $250,000 (not paid)
- Dawson County, Ga.: April 2018. Ransom demanded: $98,000 (not paid)
- (NOTE: Ransom demands were generally made in bitcoin, and some dollar amounts represent calculations that jurisdictions made to approximate the demand in dollars.)

Should Cities Pay?

Officials in Leeds , Ala., recently folded when faced with a ransom demand from hackers who froze the Birmingham suburb's computer system. It wasn't an easy choice, but everything from email to personnel records was effectively locked down, and the city of about 12,000 felt powerless.

"You just hold your nose and do it," Mayor David Miller said.

After being paid, the hackers provided a code that helped the city regain access to most of its files, he said. Similarly, Montgomery County, Ala., unable to access backup files that were also encrypted, spent about $47,000 to acquire nine bitcoins for hackers so they would unlock files last September, said Lou Ialacci, county IT director.

Every victim asks the same question, said Jeffrey Carpenter, director of incident response at SecureWorks Corp. , an Atlanta-based cybersecurity firm: "Should we pay the ransom?"

Compared with private companies, local governments may be less prepared for an attack, according to security experts. Some smaller entities can't afford to compete for cybersecurity talent, which is in high demand across the country. Information-security analysts' salaries average $100,000 a year, and private-sector employers pay more than state and local governments, according to the Bureau of Labor Statistics.

Ransoms might be loosely calibrated to what hackers think a city can pay, although numbers can vary widely. Hackers demanded $250,000 late last year from Spring Hill, Tenn., a city of

about 38,000, which is nearly five times the amount hackers tried to pilfer from Atlanta in March. Both cities refused to pay.

In Spring Hill, that has meant a still-unfolding restoration effort that could cost some $100,000, City Administrator Victor Lay said.

The St. Louis Public Library spent almost $200,000 on system upgrades after successfully fending off a ransomware demand for about $25,000 in bitcoin last year, executive director Waller McGuire said.

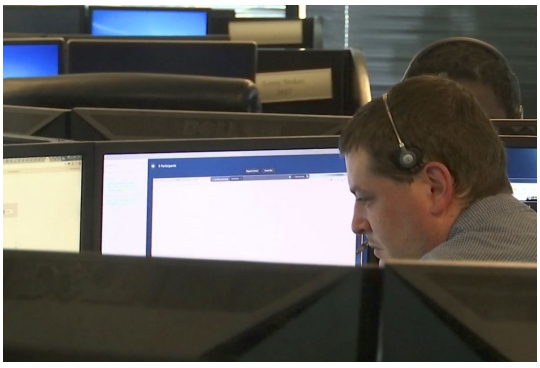
Licking County, Ohio, also refused payment when hackers demanded $50,000 in bitcoin after hijacking the county's computer system last year, apparently by exploiting a firewall gap, said County Commissioner Tim Bubb.

The county of about 170,000 people east of Columbus was lucky: Technicians quickly determined nearly all data were backed up and systems could be restored. Outside consultants also advised against paying, Mr. Bubb said.

"We didn't want to deal with criminals if we could avoid it," Mr. Bubb said. "Nobody likes to be blackmailed."

Cybersecurity Insurance: Cost vs. Benefits

Speaking at the recent mayors' conference, Atlanta Mayor Keisha Lance Bottoms triggered murmurs in a roomful of mayors when she said her city had purchased cyber insurance just months before getting hit.



Employees working in the offices of Secureworks in Atlanta in 2017. PHOTO: MARINA HUTCHINSON/ASSOCIATED PRESS

She estimated that the city, which decided to rebuild its systems, was facing more than $20 million in costs, but she hoped insurance would cover much of that. An Atlanta spokesman said the city was still evaluating the overall cost of the attack and the city's recovery efforts.

Franklin County, Ohio, the state's most populous with 1.3 million residents, bought a $10 million policy last year that came with a $200,000 annual premium. The county hasn't needed the insurance, but officials said they were motivated after seeing hackers cause disruptions in Ohio and beyond.

Some officials said they preferred to spend money on better system back-ups, since insurance wouldn't solve the immediate problem of accessing data they need to serve the public.

In Leeds, Ala., February's breach came just a week before a planned upgrade to better protect backup data, Mr. Miller said.

Insurance covered most of Leeds's ransom payment—plus, the city managed to bargain the hackers down from $12,000.

"We said, how about $8,000?" Mr. Miller recalled. "They said OK."

Write to Jon Kamp at jon.kamp@wsj.com and Scott Calvert at scott.calvert@wsj.com

Appeared in the June 25, 2018, print edition as 'Cyberattacks Target Local Governments Ransom Requests.'