Ransomware Attacks Are Testing Resolve of Cities Across America

nytimes.com/2019/08/22/us/ransomware-attacks-hacking.html

Manny Fernandez, David E. Sanger, Marina Trahan Martinez August 22, 2019

Continue reading the main story

HOUSTON — At the public library in Wilmer, Tex., books were checked out not with the beeps of bar code readers but with the scratches of pen on notebook paper. Out on the street, police officers were literally writing tickets — by hand. When the entire computer network that keeps the small town's bureaucracy afloat was recently hacked, Wilmer was thrown into the digital Dark Ages.

"It's weird," said Jennifer Dominguez, a library assistant. "We've gone old school."

This has been the summer of crippling ransomware attacks. Wilmer — a town of almost 5,000 people just south of Dallas — is one of 22 cities across Texas that are simultaneously being held hostage for millions of dollars after a sophisticated hacker, perhaps a group of them, infiltrated their computer systems and encrypted their data. The attack instigated a statewide disaster-style response that includes the National Guard and a widening F.B.I. inquiry.

More than 40 municipalities have been the victims of cyberattacks this year, from major cities such as Baltimore, Albany and Laredo, Tex., to smaller towns including Lake City, Fla. Lake City is one of the few cities to have paid a ransom demand — about $460,000 in Bitcoin, a cryptocurrency — because it thought reconstructing its systems would be even more costly.

In most ransomware cases, the identities and whereabouts of culprits are cloaked by clever digital diversions. Intelligence officials, using data collected by the National Security Agency and others in an effort to identify the sources of the hacking, say many have come from Eastern Europe, Iran and, in some cases, the United States. The majority have targeted small-town America, figuring that sleepy, cash-strapped local governments are the least likely to have updated their cyberdefenses or backed up their data.

Beyond the disruptions at local city halls and public libraries, the attacks have serious consequences, with recovery costing millions of dollars. And even when the information is again accessible and the networks restored, there is a loss of confidence in the integrity of systems that handle basic services like water, power, emergency communications and vote counting.

“The business model for the ransomware operators for the past several years has proved to be successful,” said Chris Krebs, the director of the Department of Homeland Security’s Cybersecurity and Infrastructure Security Agency, which has the primary responsibility for aiding American victims of cyberattacks.

“Years of fine-tuning these attacks have emboldened the actors, and you have seen people pay out — and they are going to continue to pay out,” he said, despite warnings from the F.B.I. that meeting ransom demands only encourages more attacks.

In Georgia alone in recent months, the tally of victims has been stunning: the city of Atlanta. The state’s Department of Public Safety. State and local court systems. A major hospital. A county government. A police department for a city of 30,000 people.

The Department of Public Safety was hit particularly hard and continues to feel the effects of an attack discovered on July 26. The computer network remains down. Every device, including laptops and tablets, is being examined and reconfigured. Much of the email system cannot be entered. State troopers are unable to use computer systems in their patrol cars; like their colleagues in Wilmer, they are writing out tickets.

[When Ransomware Cripples a City, Who’s to Blame? This I.T. Chief Is Fighting Back]

An F.B.I. warning sent to key players in the American cyberindustry on Monday left unclear who was responsible for the malware afflicting Texas, a strain first seen in April and named Sodinokibi. On Wednesday, the Department of Homeland Security issued a warning about a “Ransomware Outbreak,” cautioning cities and towns to “back up your data, system images and configurations” and keep them offline. It urged them to update their software — something Baltimore had failed to do.

Ransomware is hardly new, but it is in fashion.

A decade ago the most prevalent type of cybercrime was intellectual property theft — the stealing of industrial designs or military secrets. The American-Israeli attacks on Iran's nuclear centrifuges brought a different kind of attack to the fore: destruction of infrastructure, which has taken many forms in recent years. But ransomware is different because it does not destroy data or equipment. It simply locks it up, making it inaccessible without a complex numeric key that is provided only to those who pay the ransom.

Image
Two Iranian hackers were charged in November in connection with a ransomware attack that targeted hospitals and cities including Atlanta.Credit...Jose Luis Magana/Associated Press
Two years ago such attacks were still relatively rare. But now they are far more targeted, and as companies and towns have shown an increased willingness to pay ransoms, criminals have turned to new and more powerful forms of encryption and more ingenious ways of injecting the code into computer networks. Only this summer did the United States begin to see multiple simultaneous attacks, often directed at government websites that are ill-defended.

In the 22 Texas attacks, according to several experts who have been called in, the pathway appeared to be through a once-trusted communications channel often used by law enforcement agencies, and managed by a private systems-management firm. Getting inside a channel shared by so many Texas localities meant the hackers had to target only one system, which ushered them into municipal networks across the state. Once inside, it was fairly easy to deploy software that encrypts a town's data.

Fearing the worst, cities like Lake City, Fla., have bought cyberinsurance, and an insurer paid most of its ransom this summer. But some experts think that is only worsening the problem. Kimberly Goody, a manager of financial crimes analysis for FireEye, a major cybersecurity firm, said she expected in the future to "see some evidence that there is specific targeting of organizations that have insurance." FireEye has responded to twice as many ransomware attacks this year compared with 2018, she said.

According to government and private experts, the ransomware business is now proving so lucrative that the hackers are pouring some of their profits back into their own research and development, making their attacks more precise, and more wily.

"We are seeing more ransomware attacks because they work," said Eli Sugarman, who directs the Hewlett Foundation's cybersecurity program. "Cities are struggling to secure their complex and oftentimes outdated systems, and when attacked some choose to pay." And, he noted, there is "notoriety that comes from each successful attack."

When companies are hit with ransomware attacks they often cover it up. But cities cannot — as Atlanta learned in March 2018, in one of the most serious cyberattacks against an American municipality. Attackers demanded roughly $51,000 in Bitcoin but, according to The Atlanta Journal-Constitution, the city refused to pay the ransom. A document leaked to local

news outlets showed that responding to the attack could cost the city $17 million. At the time, Mayor Keisha Lance Bottoms called the attack “a hostage situation,” and threat researchers working on the response blamed a hacking crew called SamSam.

Two Iranians, Faramarz Shahi Savandi and Mohammad Mehdi Shah Mansouri, were indicted on a charge in that attack last year, and there has been no major recurrence of SamSam attacks since. But new, more targeted malware has appeared.

The hackers who disabled Baltimore city computers in May demanded about $76,000 in Bitcoin to release the city’s files and allow employees to regain access to their computers. The mayor, Bernard Young, said the city would not pay the ransom, in part because there was no guarantee the files would be unlocked.

In the nearly four months since, the city has brought systems back online one by one, spending more than $5.3 million on computers and contractors brought on to help recover from the attack. An early estimate put the combination of lost revenue and city expenditures at more than $18 million.

Lester Davis, a spokesman for the mayor, said some lost revenue had been recouped and that it was impossible to quantify how much money the city lost by lack of productivity and missing payments. Baltimore issued water bills in recent weeks for the first time since the hacking, meaning many residents are facing payments three times as much as normal.

Five states — California, Connecticut, Michigan, Texas and Wyoming — appear to have laws that refer specifically to “ransomware” or computer extortion, although other states have laws that prohibit extortion and computer crimes such as malware or computer trespass, according to the National Conference of State Legislatures.

Because most of the ransomware laws have been in place for only a few years, prosecutors, court officials and lawmakers say prosecutions have been nearly nonexistent.

Image
Municipal records in a vault in Lake City, Fla., which paid a ransom of about $460,000 because reconstructing its systems might have been more expensive.Credit...Eve Edelheit for The New York Times
Steve Stafstrom, House Chairman of the Connecticut General Assembly’s Judiciary Committee, said the state had enacted its ransomware law in 2017.

While no one in the state has been charged with the crime, Mr. Stafstrom said the law gave prosecutors the ability to pursue either traditional extortion charges or those specifically related to ransomware. Those convicted would face up to three years in prison.

The coordinated attack in Texas began on Friday morning. State officials said a “single threat actor,” which could be a group, was behind the cyberattack, but they declined to elaborate or discuss details about how the virus spread, referring questions to the F.B.I. office in Dallas,

which also declined to release details of its investigation.

Four of the 22 towns have a total of about 31,000 residents. Such small city governments, which often use motley collections of vintage software and lack the budget and sophistication for strong cyberdefense, have become a favorite target for ransomware attacks.

Last year, hackers based in Ukraine hit Allentown, Pa., a city of 121,000 residents, with a malware package that shut down the city government's computers for weeks. No explicit ransom demand was made, but the attack played out like many that target cities, said Matthew Leibert, Allentown's longtime chief information officer.

When an Allentown city employee took a laptop with him while traveling, it missed software updates that might have blocked the malware. The employee unwittingly clicked on a phishing email, and when he returned to the office, the malware spread rapidly.

The attack cost about $1 million to clean up, Mr. Leibert said. Improved defenses are costing Allentown about $420,000 a year, squeezing the city's budget. He said one frustration was the scattershot targeting that happened to hit Allentown. "There are warehouses of kids overseas firing off phishing emails," Mr. Leibert said.

Although some of the Texas towns' computer systems are now back online, others are being restored by teams of state and federal cybersecurity experts and investigators, including those with the National Guard in Texas. In Wilmer, a team of National Guard specialists arrived Friday, dressed in T-shirts in the August heat and using the police station as its headquarters. They continue to work restoring the network and recovering data.

In Kaufman, located more than 30 miles southeast of Dallas, city employees were forced to conduct business manually instead of through computers. City staff members used their cellphones because the phone system was disabled.

Mike Slye, Kaufman's city manager, said he was not permitted to discuss details of the attack, including how it was discovered.

Such a response is typical in the aftermath of small-town cyberattacks. Some local leaders are embarrassed, while others fear that by discussing the attack, they will invite future ones or will expose a weakness in their cyberdefenses.

Officials in Wilmer hoped to have the city's systems fully operational in two to three weeks. The mayor, Emmanuel Wealthy-Williams, issued a statement as well.

It was neatly handwritten, on notebook paper.