Bond Case Briefs

Municipal Finance Law Since 1971

Ransomware Attacks Demanding Larger Payouts from Local Governments.

The average ransom demanded of a local government in a cyberattack grew from $30,000 to $380,000, according to one cybersecurity firm.

Hackers carrying out ransomware attacks against local governments are demanding larger sums of money and finding that smaller municipalities are willing to pay up, according to cybersecurity experts.

The ransom demands made on local governments after computer systems are breached or private data is stolen have increased from an average of $30,000 in 2017 to $380,000 in 2019, according to a report published this month by BlueVoyant cybersecurity firm. Several ransom demands exceeded $1 million last year.

The increased monetary demands reflect a shift in technique among hackers, according to the report. Ransomware attacks on local governments were previously opportunistic in nature, exploiting vulnerabilities for the possibility of a quick payout. But more recent attacks are "targeted ransomware intrusions focused on larger organizations, with critical digital services, that could be ransomed for high amounts," the BlueVoyant report states.

The firm analyzed 108 attacks on state and local governments going back to 2017 to better understand cybersecurity issues facing local governments.

Another report, released Thursday, found that the number of ransomware attacks affecting local governments has decreased over the last 12 months. The cybersecurity company Barracuda found that hackers made ransom demands against 33 municipal governments in the last 12 months compared to 55 attacks the year before.

But smaller municipalities have come under increasing attack as hackers exploit their vulnerabilities and lack of resources, said Fleming Shi, the chief technology officer of Barracuda. At least 15% of the 33 municipalities attacked in the last 12 months paid the demanded ransom, with payments ranging from $45,000 to $250,000, the Barracuda report found.

"All the municipalities studied that made payments had populations less than 50,000, and they deemed the cost and labor associated with manually recovering from the ransomware attacks too high," the Barracuda report states. "That's a significant change compared to last year, when practically none of the municipalities attacked paid any ransom."

While prior ransomware attacks have often centered on locking government officials out of their own computer systems and demanding payment to let them back in, Shi said hackers now more likely steal private information from local governments and to demand payment not to release it.

"Data breaches and exposing very private or critical data is becoming part of their tactic," he said.

To protect themselves from ransomware attacks, the BlueVoyant report recommends local governments conduct cybersecurity risk assessments and consider purchasing cyber insurance or working with a managed security service.

Managed service providers have increasingly come to the aid of smaller municipalities to help them recover their data or restore access to computer systems, Shi said.

“Without any help, they are likely to pay because they don’t have the infrastructure to remediate or recover data,” Shi said.

Andrea Noble is a staff correspondent with Route Fifty.

Route Fifty

By Andrea Noble

AUGUST 27, 2020