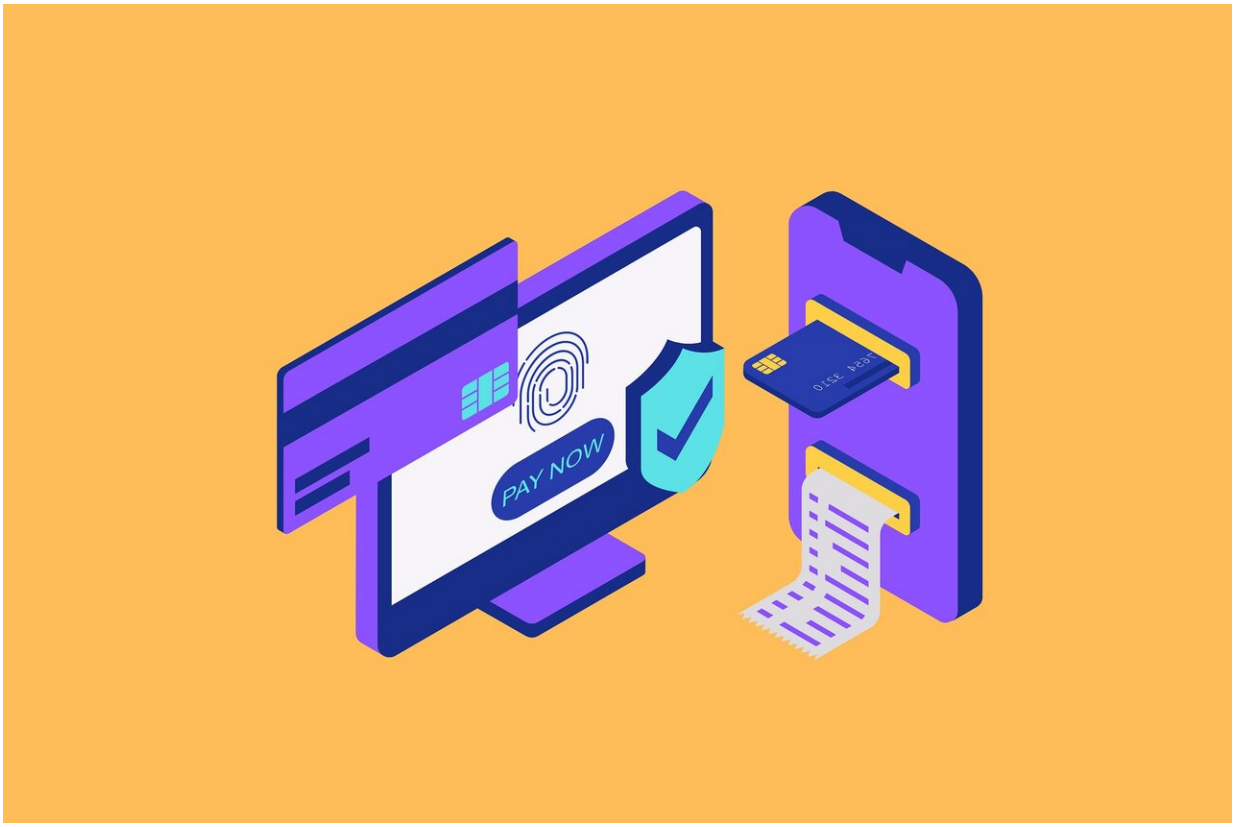
Large Florida school district hit by ransomware attack

April 1 2021, by Terry Spencer and Frank Bajak



Credit: Pixabay/CC0 Public Domain

The computer system of one of the nation's largest school districts was hacked by a criminal gang that encrypted district data and demanded $40 million in ransom or it would erase the files and post students' and

employees' personal information online.

Broward County Public Schools said in a statement Thursday that there is no indication that any personal information has been stolen and that it made no extortion payment to the ransomware gang, which as an apparent pressure tactic last week posted screenshots of its online negotiations with the district to its site on the dark web.

The Fort Lauderdale-based district said it is working with cybersecurity experts "to investigate the incident and remediate affected systems. Efforts to restore all systems are underway and progressing well. We have no intention of paying a ransom." The district did, after two weeks of back and forth, offer to pay $500,000, at which point the ransomware criminals apparently ended negotiations, according to the hackers' screenshots.

The district declined further comment outside its statement. With 271,000 students, Broward is the nation's sixth-largest school district with an annual budget of about $4 billion—a fact the hackers kept returning to as they demanded $40 million, to be paid in cryptocurrency. The ransomware caused a brief shutdown of the district's computer system in early March, but classes were not disrupted.

"It is a possible amount for you," the Conti gang said early in its negotiations with a district official, whose name does not appear in the screenshots and has not been released. Its data-locking malware is one of the top 10 strains of ransomware.

"This is a PUBLIC school district," the Broward negotiator replied. "You cannot possibly think we have anything close to this!" It was unclear if the representative was a district employee or, as is often the case, a hired ransomware negotiator.

The FBI usually investigates such attacks, but said Thursday it would not confirm if it was investigating this one.

An epidemic of ransomware attacks has been plaguing government agencies, businesses and individuals for the past three years. Most are Russian-speaking gangs based in Eastern Europe and enjoy safe harbor from tolerant governments. The more sophisticated groups identify their targets in advance, infect networks through phishing or other means and often steal data as they plant malware that encrypts a victim's network.

After the ransomware is activated, the criminals demand money to unlock the malware and refrain from posting—or selling—stolen data. In the case of corporations, that data could be trade secrets. In the case of retailers or government agencies it could be Social Security, bank account numbers and birth dates.Conti claimed it stole from Broward's system Social Security numbers, birth dates and other student and employee information.

Public school districts have been frequent targets of ransomware attacks. The districts of Baltimore County, Maryland; Fairfax County, Virginia; Hartford, Connecticut; and Fort Worth, Texas, were among those hit last year. Elementary, middle and high schools have been increasingly targeted in recent months, according the the Cybersecurity and Infrastructure Security Agency. In December, it said that K-12 schools accounted for 57% of all reported attacks in August and September as compared to 28% for January through July.

Overall, ransomware attacks disrupted learning at 1,681 schools, colleges, and universities in 2020 and at least 544 so far this year, said analyst Brett Callow at Emsisoft, a cybersecurity firm. Seven districts had personal data published.

Many ransomware cases go unreported due to the liability and stigma

attached to victims. Cybersecurity firms have good data on ransoms paid in part because negotiations between victims and hackers occur on dark websites that researchers learn about through shared malware samples where criminals typically leave ransomware notes with instructions and demands. An entire subindustry has also emerged to help victims manage the emergencies.

The average ransom paid for to hacking gangs nearly tripled from $115,000 in 2019 to $312,000 in 2020, according to the cybersecurity firm Palo Alto Networks. It said the highest ransom paid by an organization doubled last year from to $10 million, up from $5 million in 2019.

In Conti's negotiations with Broward, after the gang's initial $40 million demand, it said it was willing to negotiate: it would accept $15 million in Bitcoin but it had to be delivered within 24 hours. Otherwise, it would upload the personal information it claimed to have and permanently lock the computer system. Conti said legal claims against the district for losing the data would exceed $50 million, so it should consider its demand a bargain.

"Pay $15M and you guys are guaranteed to solve your problem," Conti told the district.

The district insisted it still couldn't afford it and, in any case, didn't have access to Bitcoin. Ransomware gangs demand payment in cybercurrency because it can be difficult to trace.

Conti upped its threat by suggesting it had found damaging information about an unnamed royal family in Broward's database—an allegation the district's negotiator found absurd.

"What do you mean about a royal family ... we are a public school

district," the negotiator replied.

The negotiations continued for two weeks, with Conti eventually lowering its demand to $10 million. The district made its $500,000 counteroffer. That is the last screenshot posted.

"The negotiation is bizarre," said Callow, the Emsisoft analyst. "The Conti operators are experienced extortionists, so it's odd that they seemed not to know who they were dealing with and demanded an amount that a public school district was never likely to pay. I can't explain it."