Ransomware gang wanted $40 million in Florida schools cyberattack

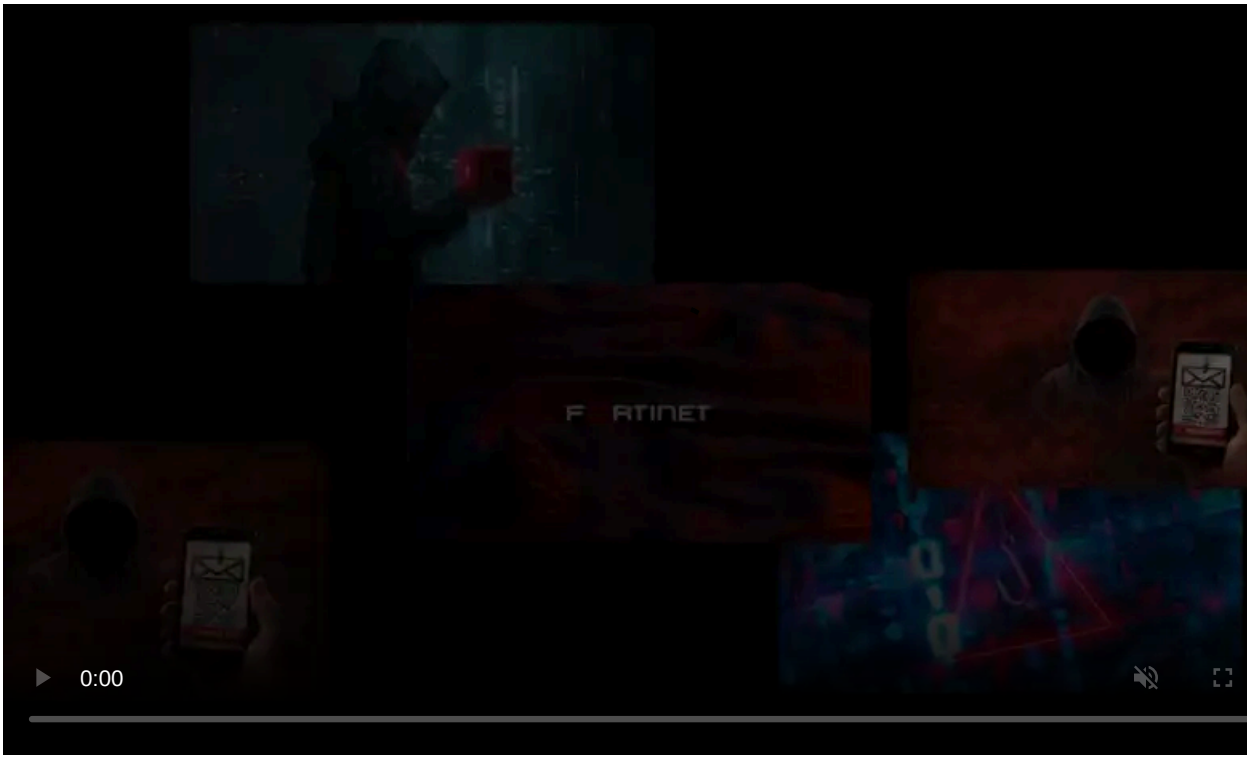
By Lawrence Abrams

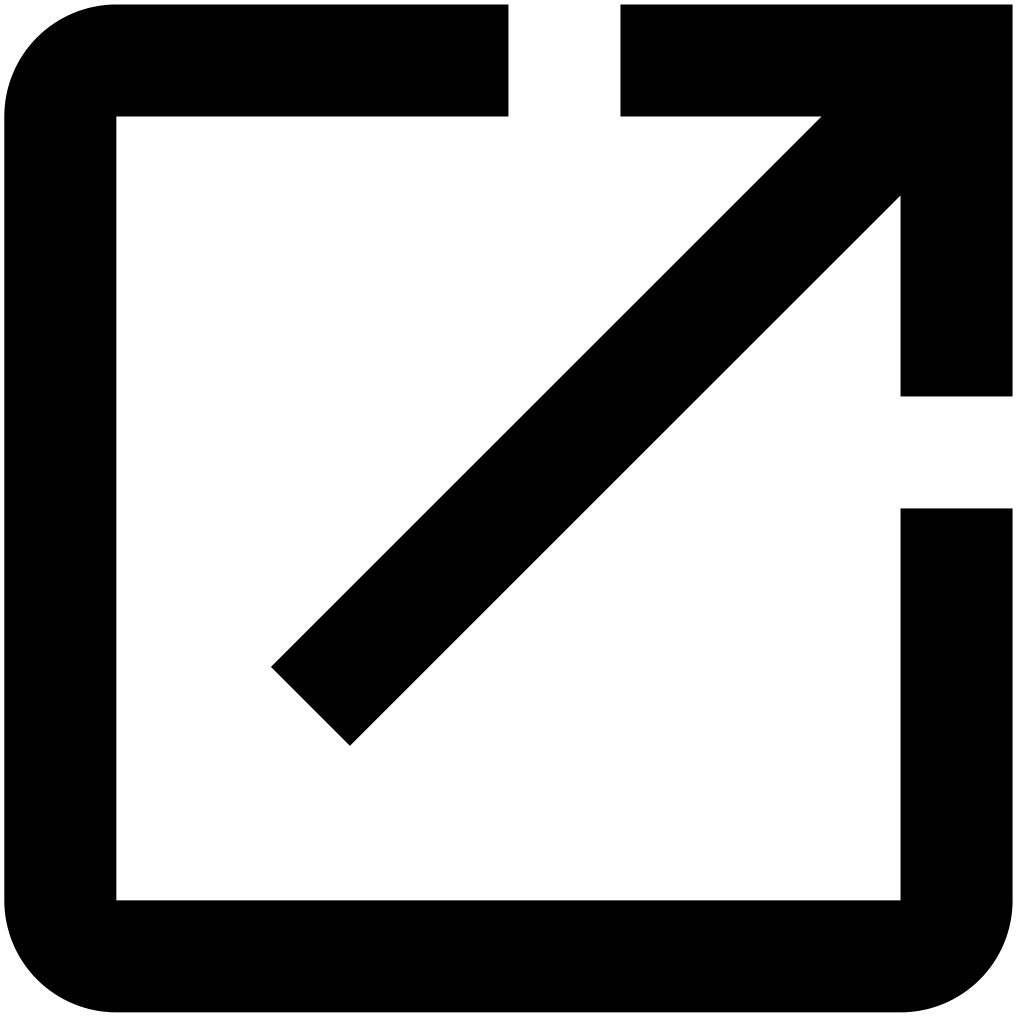
Published: 2021-04-02 · Archived: 2026-04-06 00:27:02 UTC

Fueled by large payments from victims, ransomware gangs have started to demand ridiculous ransoms from organizations that can not afford to pay them. An example of this is a recently revealed ransomware attack on the Broward County Public Schools district where threat actors demanded a $40,000,000 payment.

According to the Broward County Public Schools (BCPS) website, the school system is the sixth-largest in the USA, with nearly 261,000 students and approximately 110,000 adult students in 241 schools, centers, and technical colleges, and 92 charter schools.

Last month, Florida's Broward County Public Schools had to shut down their IT systems after suffering what was reported as a cyberattack. Since then, the school system has not disclosed any further information regarding the attack.

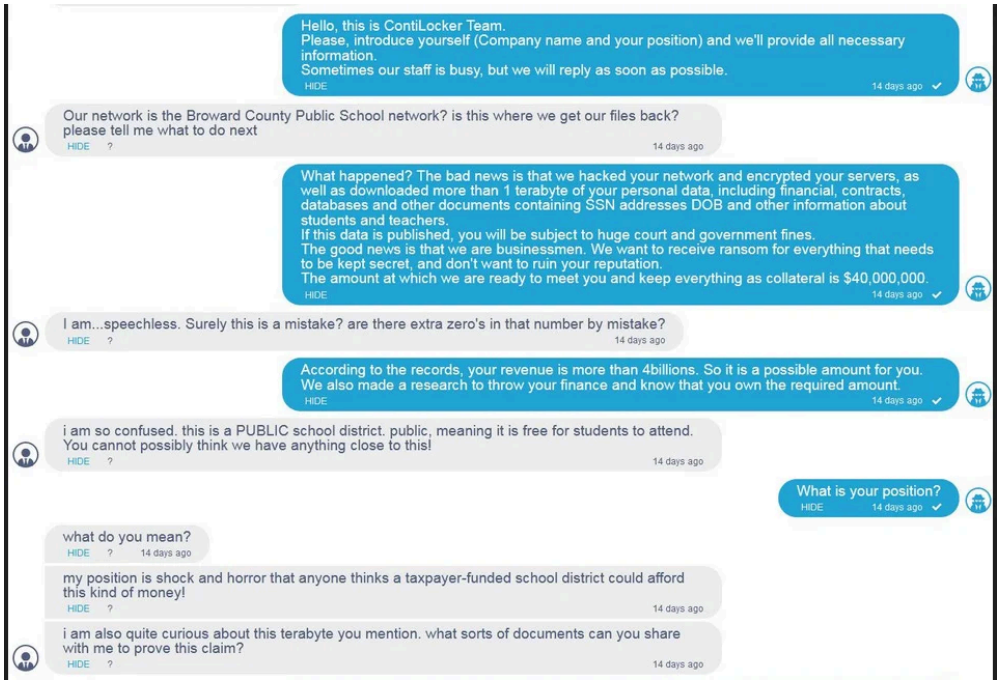

F RTINET
0:00



As first reported by databreaches.net, this week, a ransomware gang known as Conti has claimed responsibility for the attack. After negotiations failed, the threat actors published alleged screenshots of the ransom negotiation from Broward County Public Schools' attack.

These screenshots revealed that the threat actors initially demanded a $40,000,000 ransom from the district, which left the BCPS representative shocked that the threat actors thought they could afford that much money.

This is illustrated in a snippet of the conversation between a BCPS representative and the Conti gang, shown below.



Alleged ransomware negotiations published by Conti

According to the screenshots of the negotiation process, the ransom was ultimately lowered to $10 million, but it was still far more than the $500,000 the school district was willing to pay. This led to the end of the negotiations and the screenshots being posted.

From the numerous ransomware negotiations seen by BleepingComputer, ransomware gangs always pride themselves on researching a victim's finances before setting a ransom amount. They then try to throw this financial information in the face of the victim while negotiating.

They also tend to start with high ransom amounts, knowing that the negotiation process will significantly whittle down the ultimate payment.

While a corporate victim's financial information can be gleaned from revenue reports, stolen data, or even insurance policies, it appears they failed to understand that public school systems in the USA typically operate on a tight budget.

Furthermore, schools have had to dip into their cash reserves to open schools under strict health guidelines due to the pandemic, leaving little room for million-dollar ransom payments.

When a public school has to take money away from their budget for an unexpected expense, it is the students who suffer, and it is ultimately the tax payer who bears the cost of paying these ransoms.

While ransomware gangs have successfully extorted public schools and universities in the past, it is not nearly as common as with the enterprise.

The $40 million ransom in the Broward County Public Schools cyber attack is the second-most largest demand seen to date. The largest ransom is from REvil on their attack against Acer, where the attackers demanded $50 million.
